UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

2013-1682

FINJAN, INC., a Delaware corporation,

PLAINTIFF-APPELLANT,

V.

SYMANTEC CORP., a Delaware corporation, WEBSENSE, INC., a Delaware corporation, SOPHOS, INC., a Massachusetts corporation,

DEFENDANTS-APPELLEES.

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE IN CASE NO. 10-CV-593-GMS, Judge Gregory M. Sleet

BRIEF FOR PLAINTIFF-APPELLANT FINJAN, INC.

PAUL J. ANDRE
LISA KOBIALKA
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 MARSH ROAD
MENLO PARK, CALIFORNIA 94025
TEL: (650) 752-1700

JEFFREY M. HARRIS
BANCROFT PLLC
1919 M STREET, NW
SUITE 470
WASHINGTON, DC 20036
TEL: (202) 234-0090

ATTORNEYS FOR PLAINTIFF-APPELLANT
FINJAN, INC.

CERTIFICATE OF INTEREST

Counsel for Plaintiff-Appellant, Finjan, Inc., certifies the following:

1. The full name of every party represented by us is:

   Finjan, Inc.

2. The name of the real party in interest represented by us is:

   Finjan, Inc.

3. All parent corporations and any other publicly held companies that own 10 percent or more of the stock of the party or *amicus curiae* represented by me are:

   Finjan Holdings, Inc. owns 100% of the stock of Finjan, Inc. No parent corporation or publicly held company holds 10% or more of the stock of Finjan Holdings, Inc.

4. The names of all law firms and the partners or associates that appeared for Finjan, Inc. in trial court or are expected to appear in this court are:

   Paul J. Andre, Lisa Kobialka, James Hannah, Aaron M. Frankel and Hannah Lee of Kramer Levin Naftalis & Frankel LLP.

   Philip A. Rovner of Potter Anderson & Corroon LLP.

   Jeffrey M. Harris of Bancroft PLLC.

Dated: December 10, 2013

/s/Paul J. Andre
Paul J. Andre
Lisa Kobialka
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, California 94025
Tel: (650) 752-1700
Fax: (650) 752-1800

Attorneys For Plaintiff-Appellant
Finjan, Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF RELATED CASES

Pursuant to Fed. Cir. Rule 47.5(a), Finjan, Inc. ("Finjan") states that no appeal other than the current appeal has been taken in or from the same civil action or proceeding in the District Court.

Pursuant to Fed. Cir. Rule 47.5(b), Finjan states that it and Websense, Inc. are parties to *Finjan, Inc. v. Websense, Inc.*, 3:13-cv-04398 (N.D. Cal. Sept. 23, 2013). There are no other pending cases between the parties to this appeal.

STATEMENT OF JURISDICTION

Chief Judge Gregory M. Sleet of the United States District Court for the District Court of Delaware (the "District Court") had jurisdiction over Finjan's patent infringement action below under 28 U.S.C. §§ 1331 and 1338.

On December 21, 2012, the District Court entered final judgment in favor of Defendants-Appellees Symantec Corp. ("Symantec"), Websense, Inc. ("Websense") and Sophos Inc. ("Sophos") (together, "Defendants") after the conclusion of a jury trial. JA1-2.

On September 19, 2013, the District Court issued a Memorandum Opinion denying Finjan's Motion For a New Trial and Renewed Motions for Judgment as a Matter of Law ("JMOL") against Defendants (the "Opinion"). JA110.

Finjan filed a timely notice of appeal on September 25, 2013. JA14502-06. This Court has jurisdiction over this appeal under 28 U.S.C. § 1295.

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

The issue presented in this appeal is whether the District Court erred in allowing to stand the jury's verdict that U.S. Patent Nos. 6,092,194 and 6,480,962 (the "Asserted Patents") are invalid. More specifically:

1. Did the District Court err in denying Finjan's Motions for JMOL that the Asserted Patents are not invalid where Defendants failed to submit substantial evidence satisfying their clear and convincing burden of proof that the asserted prior art disclosed all of the limitations of the asserted claims (as properly construed) including the inventive runtime behavioral analysis protection?

2. Did the District Court err in denying Finjan's Motion for a New Trial in view of:

(a) the District Court's substantial error in precluding Finjan's validity expert from testifying regarding his review of machine code that provided the foundation for his opinions, enabling Defendants to severely Prejudice Finjan's validity case by incorrectly arguing to the jury that Finjan's validity arguments were unfounded;

(b) the facial inconsistency in the jury's verdict in finding that early versions of Sophos' accused products invalidated the asserted claims but the accused versions do not infringe, even though Sophos conceded infringement and argued that the earlier and accused products both fell within the scope of the asserted claims; and

(c) the jury verdict of invalidity being against the clear weight of the evidence?

STATEMENT OF THE CASE

Finjan brought this action in the United States District Court for the District of Delaware alleging that Defendants infringe certain claims of the Asserted Patents, which are directed to methods and systems for protecting computers and networks from malicious software. After a jury trial, the District Court entered judgment that the asserted claims are invalid and not infringed by the Defendants. JA1-2. The District Court denied Finjan's post-trial Motions For a New Trial and JMOL that the asserted claims are valid and infringed by Defendants. JA110.

This appeal followed.

I. INTRODUCTION

Finjan respectfully requests that this Court reverse the jury verdict of invalidity of the Asserted Claims. The jury's findings were based on a fundamental misunderstanding of the ways in which Finjan's innovative technologies improved upon the prior art.

Prior art computer security programs, including the art asserted by Defendants at trial, were focused on identifying potentially malicious software by looking for known segments of malicious code (referred to as "signature matching"). One flaw with this approach is that such security systems could only detect threats that had already been identified and from which a signature had been extracted. These systems were incapable of identifying new threats for which no signature had been provided. Finjan's patents solved this problem by identifying threats by detecting suspicious operations ("behavioral analysis"), thus allowing for the proactive identification of previously unknown malware.

Finjan's patents also represent a significant improvement over the prior art in addressing the threat posed by downloading and running scripts over the Internet. Prior art security systems were focused on periodically inspecting files after they had been downloaded onto a local computer's file system. Finjan recognized the threat posed by files downloaded from the Internet, and especially by script-based programs (such as JavaScript and Visual Basic) that are downloaded and executed by an Internet browser. The Asserted Patents teach inspecting such script-based threats for suspicious behaviors and provide for runtime monitoring of multiple subsystems (not just periodic inspections of local file systems), especially network subsystems. As these concepts are not disclosed in the prior art, no reasonable jury could have found the Asserted Claims invalid.

In the alternative, a new trial is warranted. The District Court completely undermined the credibility of Finjan's validity expert and validity case when it precluded foundational testimony regarding the reliability of that expert's analysis of the prior art. Because of confidentiality restrictions, Finjan's expert was allowed to analyze only the machine executable code for the prior art, not the source code. During cross-examination, Defendants repeatedly suggested that reliance on machine code alone was inadequate. Finjan attempted to rehabilitate its expert on re-direct by introducing testimony showing that machine code is highly instructive in demonstrating how a program actually operates. Remarkably, the District Court barred this testimony *sua sponte* based on the mistaken belief that Finjan's expert had not addressed this issue during his examination. And Defendants then seized upon this mistake by arguing as a major theme in closing argument that Finjan's validity theories should be rejected because Finjan's expert supposedly was unfamiliar with the actual operations of the prior art. This was plainly not the case, and the District Court's erroneous exclusion of this testimony irreparably tainted the jury's deliberation on validity.

A new trial is also necessary in view of the facial inconsistency in the jury's verdict. Sophos' core defense was that prior art versions of its current products fell within the scope of the Asserted Claims, and thus invalidated Finjan's patents. Sophos did not attempt to distinguish its current products from the prior art and, indeed, conceded infringement of its accused products. It was thus a logical impossibility for the jury to find *both* invalidity based on the prior art and non-infringement of Sophos' accused products. Yet the jury found just that. This irreconcilably inconsistent verdict requires a new trial.

II. STATEMENT OF FACTS

A. The Parties and the Accused Systems

1. Plaintiff Finjan

Finjan was founded in 1996 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation, to develop security software that protects computer data and networks through content analysis. JA7027, 498:12-14; JA7031-32, 513:7-516:15. Since its formation, Finjan has invested more than a decade of research and development into its inventions, built and sold products around the world, and committed tens of millions of dollars to research and development.

Specifically, Finjan was the pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats recognized today under the umbrella of "malware." These technologies protect networks and endpoints by identifying suspicious patterns and behaviors within Internet-delivered content. Finjan's inventions were revolutionary compared to traditional—signature matching—anti-virus technologies in that they performed proactive, behavioral analysis, which allowed detection and blocking of *unknown* threats. In contrast, traditional signature-matching security products could only block known malware. JA7030, 508:12-25; JA7032, 518:12-519:6; JA7033-34, 521:9-524:21; JA7055, 529:24-530:16.

Finjan was the first security company to recognize the emerging threat presented by the Internet, which allowed for rapid downloading and execution of script-based files; in contrast, the prior art was focused on periodically inspecting files already downloaded onto a local computer system. In fact, the company's name "*finjan*" means a container of coffee in the Middle East, and was chosen to symbolize Finjan's technology that allows for the safe use and containment of Java and other script-based languages. JA7030, 510:20-511:8, JA7032, 516:2-517:13.

In 1999, Finjan began selling its patented products. Finjan built and sold software, including APIs (application programing interfaces) and appliances for network security using these patented technologies. At its height, Finjan employed nearly 150 employees around the world, building and selling security products and operating the Malicious Code Research Center through which it frequently published research regarding network security and current threats on the Internet. However, by the mid-2000s, as a small company with limited resources, Finjan had difficulty competing with larger competitors in the marketplace who began moving towards the behavior-based proactive threat detection that Finjan had invented. It was at this time that Finjan began offering licenses to its intellectual property. JA7032, 517:14-518:11; JA7064, 644:18-645:4; JA7065, 649:8-650:6.

In 2009, due to the widespread use by others of its behavior-based inventions, Finjan was forced to move its sales and marketing efforts to a larger technology company, M86 Security, Inc. ("M86"). JA7065, 650:7-18. Currently, Finjan is a technology company applying its research and expertise with security technologies to working with inventors, investing in and/or acquiring other technology companies, investing in a variety of research organizations, and evaluating strategic partnerships with companies offering security-related products.

2. Defendants

Defendant Symantec is a computer security company that makes and sells security products that operate at both the network access point/gateway

("Matrix") and client-side/endpoint ("BASH" or "Sonar"), and that include proactive, behavioral technology to detect malware. JA7197, 726:4-24.

Defendant Sophos is a computer security company that also makes and sells both gateway and client-side malware detection products that include proactive, behavioral technology (respectively, "Behavioral Genotype technology" and "HIPS runtime technology"). JA7319, 1074:4-20.

Defendant Websense makes and sells computer security products called Websense Security Gateway, Websense Security Gateway Anywhere and Triton. These products contain its accused Real-Time Security Scanning proactive, behavioral technology. JA7417, 1322:1-1323:19.

B. The Asserted Patents

The core teachings of the Asserted Patents relate to systems and methods for proactively protecting computers and networks from hostile "Downloadables"—executable application programs which are downloaded from a source computer and run on a destination computer.

1. The Inventions of the '194 Patent

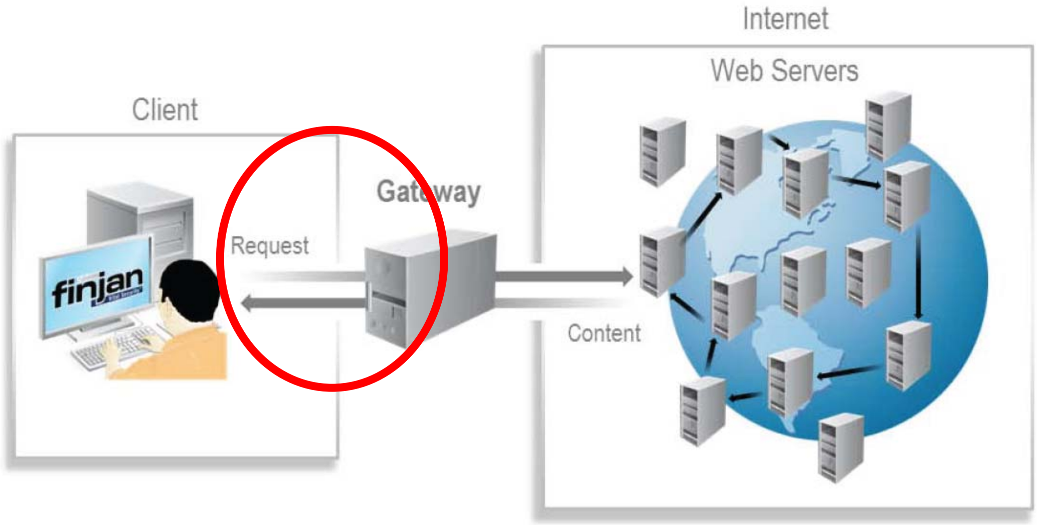
U.S. Patent No. 6,092,194 (the "'194 Patent") is entitled "System and Method For Protecting a Computer and a Network From Hostile Downloadables," and issued on July 18, 2000 to Shlomo Touboul. JA271-93. The '194 Patent was filed on November 6, 1997 and claims priority to Provisional Application No. 60/030,639, dated November 8, 1996. *Id.*

The '194 Patent discloses proactive detection of malware based on an analysis of its behavior (as opposed to just looking for known signatures defining malicious code). The asserted method and system claims of the '194 Patent disclose a "gateway server" that receives an incoming "Downloadable" file. A Downloadable "is an executable application program, which is downloaded from a source computer and run on the destination computer." A Downloadable is typically an applet or script (such as a JavaScript applet) requested by an ongoing process, for example by an Internet browser. JA283, 1:41-57.

The gateway server examines "security profile" data corresponding to the Downloadable, which must include a list of suspicious operations that may be attempted by the Downloadable. JA283, 2:11-21. A wide variety of operations can be deemed potentially hostile, including reading or writing to certain files (e.g., important system files), registry operations and operating system operations (such as starting or terminating processes). JA285, 5:58-6:4.

The gateway server then compares the security profile data (including information about operations) against a "security policy." JA285, 5:4-7:2. The security policy defines parameters that, if violated, will cause the gateway server to determine that the Downloadable is suspicious and to prevent execution of the Downloadable. *Id*.

The inventions of the ‘194 Patent generally differ from the prior art in at least two important respects. *First*, prior art antivirus programs focused only on monitoring local file systems. In contrast, the ‘194 Patent teaches a “gateway” that inspects potentially dangerous software before it is downloaded to the client (as shown in the figure below); these processes occur in different physical locations, on different equipment, across the connected network. *Second*, the prior art identified potential threats by signature matching. A flaw in this approach is the inability to detect dangerous software until it has already been identified as malicious (referred to as the “zero day problem,” because of the inability of signature matching to protect from new threats when they are first introduced). The ‘194 Patent teaches examining the actual operations of incoming files to determine if the file is malicious (known as “behavioral” detection), which allows detection of harmful software even if it has not previously been identified as malicious. JA6973, 441:5-442:7.



All claims of the ‘194 Patent were confirmed as valid by the U.S. Patent and Trademark Office (“USPTO”) after an *ex parte* reexamination request submitted by Websense asserting twelve prior art references. JA291-93. The USPTO also confirmed the claims over additional prior art submitted by Finjan. *Id.* In fact, all claims of the ‘194 Patent were allowed in the first office action before Finjan submitted a response to the USPTO.

2. The Inventions of the ‘962 Patent

U.S. Patent No. 6,480,962 (the “‘962 Patent”) is entitled “System and Method For Protecting a Client During Runtime From Hostile Downloadables,” and issued on November 12, 2002 to Shlomo Touboul. JA294-310.

The ‘962 Patent applies an additional layer of behavior-based protection to the technology of the ‘194 Patent at the endpoint (or client). JA6973, 441:15-442:7. Specifically, the asserted method and system claims of the ‘962

Patent cover monitoring multiple subsystems of the operating system, including the file management system, network management system, process system and memory system. JA304, 4:19-31.

This monitoring occurs in "runtime," i.e., while Programs are being executed. JA304, 3:41-51, 4:32-49. When a Downloadable makes a request (e.g., a read/write operation) while the Downloadable is being executed, the request is interrupted and information pertaining to the Downloadable is compared to a predetermined security policy. *Id.* This refers to information about the Downloadable itself, not just the specific request the Downloadable has made to the operating system. For example, the system may examine identifying information about the Downloadable to determine if it has already been identified as suspicious. JA304-05, 4:63-5:2. If the security policy is violated, a predetermined responsive action is taken, such as notifying the user, stopping the execution of the Downloadable or adding the Downloadable to the database of known threats. JA305, 6:14-21.

In contrast to the prior art, which was directed to monitoring file systems, the '962 Patent claims monitoring a *plurality* of subsystems, rather than a single subsystem, and especially network systems (recognizing the importance of Internet-based threats). JA8858-59, 3024:9-3027:20. In addition, the '962 Patent focuses on the source of the suspicious operations, rather than just the target of the request (e.g., certain operations may be acceptable if they originate from one source, but might trigger a response if they originate from a more suspicious source). JA8859, 3027:21-3029:4.

All claims of the ‘962 Patent were confirmed by the USPTO over prior art asserted by Websense in an *ex parte* reexamination (as well as additional prior art submitted by Finjan). JA309-10.

C. Prior Assertions and Licensing of the Asserted Patents

Both the courts and the marketplace have concluded that Finjan’s patents are valid, enforceable and valuable. Prior to the instant action, Finjan successfully asserted several patents, including the ‘194 Patent, against Securing Computing Corporation, Cyberguard Corporation and Webwasher AG, resulting in a jury verdict that all of the patents were valid and that Defendants willfully infringed Finjan’s patents. *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1200 (Fed. Cir. 2010). This Court affirmed defendants’ infringement of Finjan’s system and storage medium claims and the damages award (while finding noninfringement of the asserted method claims). *Id.* at 1213.

In addition to litigation-related settlements with defendants McAfee and Webroot, Finjan successfully licensed its computer security patent portfolio to others. Microsoft obtained a license to Finjan’s patent portfolio for $8 million and other consideration (including a $2 million investment in Finjan and marketing assistance). JA7036, 533:8-534:18. Microsoft took this license, even though it was not active in the security market, in order to obtain coverage for a small security company it had acquired. *Id.* After Finjan merged its product lines into M86 (while retaining its patent portfolio), M86 took a license, accounted for as the equivalent of a 7.5% running royalty. JA7521, 1594:15-1595:1. TrustWave purchased a separate license to Finjan's patent portfolio when it acquired M86, based on a 6% royalty rate on the entire market value of the licensed software. JA6362, 245:12-246:10.

D. The Proceedings Below

Finjan filed this suit on July 12, 2010 against Symantec, Sophos and Websense. JA311. The Complaint also named McAfee Inc. and Webroot Software Inc., with whom Finjan granted licenses and subsequently settled. *Id.*

1. Claim Construction Order

The District Court issued a claim construction order construing the following terms:

Term	Patent	Construction
Downloadable	'194 & '962 Patents	"an executable application program, which is downloaded from a source computer and run on the destination computer."
Downloadable security profile data pertaining to the Downloadable	'194 Patent Only	Plain and ordinary meaning.

Term	Patent	Construction
a list of suspicious computer operations that may be attempted by the Downloadable	‘194 Patent Only	Plain and ordinary meaning.
information pertaining to the Downloadable	‘962 Patent Only	Plain and ordinary meaning.

As discussed in the argument below, several terms which turned out to be dispositive on issues of validity were not construed or were only given a plain and ordinary meaning construction. For example, various claims recite that the Downloadable inspected for malicious operations “includes JavaScript script” or “Visual Basic script.” Finjan contends that this limitation is only satisfied when the JavaScript or Visual Basic code is searched for malicious operations, while Defendants contended (and the District Court agreed) that these limitations can be satisfied when a Downloadable containing JavaScript or Visual Basic script is examined for malicious operations, even if the script code itself is not examined.

2. Defendants’ Invalidity Defense

At trial, Defendants argued invalidity based on several references (the “Asserted Prior Art”). The primary grounds included: (1) a combination of version 2.72 of Sweep, a server application, and version 2.11 of InterCheck, a client-based program (both earlier versions of the accused Sophos products), (2) a combination of version 7.0 of ThunderByte and MIMESweeper (during prosecution of the ‘194 Patent, the claims issued over ThunderByte) and (3) Norton Antivirus 95 (“NAV

95") (an early Symantec product). JA8860, 3032:4-3034:1; JA8867, 3059:23-3062:8; JA8870, 3073:17-3074:2; JA8891, 3156:9-3157:7.

Over Finjan's objection, the final jury verdict form asked the jury to decide if the Asserted Claims are anticipated and obvious, but did not ask the jury to identify the specific prior art that its decision was based upon. JA7-8. Based on the arguments presented at trial, the finding of anticipation of the '194 Patent was based on Sweep-InterCheck, obviousness of the '194 Patent was based on ThunderByte and MIMESweeper and anticipation of the '962 Patent could have been based on NAV 95, Sweep-InterCheck or both. The basis of obviousness of the '962 Patent was unclear as Defendants did not present an obviousness analysis (other than for one claim). JA3-10.

The following table summarizes the invalidity arguments presented by Defendants at trial for the Asserted Claims each Asserted Patent:

Theory	'194 Patent	'962 Patent
Anticipation	(1) Sweep & InterCheck	(1) NAV 95 (Except Claim 52) (2) Sweep & InterCheck
Obviousness	(1) ThunderByte & MIMESweeper	Not Argued (Except Claim 52)

3. Jury Trial

The jury trial in this action commenced on December 3, 2012. Jury instructions were read on December 19, 2012.

During the trial, considerable emphasis was placed on the importance of source code as evidence of how software operates. *See, e.g.*, JA96 (District Court: “throughout the trial, the parties focused on the source code of the accused products and prior art products as the best evidence of how the products operate”). Defendants’ invalidity experts relied on reviews of the confidential source code for the asserted prior art. *Id*.

Due to confidentiality issues, Finjan’s expert, Dr. Vigna, could not review confidential source code and explained that he instead relied on a review of machine code for the prior art. JA8859-60, 3030:3-3031:11. During direct examination, Dr. Vigna explained that the machine code is the actual set of instructions used by the computer to execute software, and provides an even more reliable indication than source code of how software actually operates. *Id*. During cross-examination, Defendants challenged Dr. Vigna regarding the foundation for his validity opinions in view of his review of machine code instead of source code. JA8887, 3140:7-14; JA8889, 3147:14-19.

When Finjan began to address this issue during redirect examination, the District Court *sua sponte* precluded the testimony, mistakenly stating that Dr.

Vigna had not previously testified about this review. JA8892, 3159:21-3160:1. Defendants then repeatedly argued during closing argument that their experts' invalidity opinions should be credited over Dr. Vigna's because Dr. Vigna had not reviewed the source code. *See, e.g.*, JA8977, 3331:6-9; JA8979, 3339:11-21; JA8981, 3346:4-5; JA8984, 3361:8-19, 3362:23-3363:5, 3363:16-23.

During jury deliberations the jury asked the District Court if it needed to even consider Defendants' invalidity defenses if it had concluded that there was no infringement by Defendants. JA9388, 3429:1-3430:25. The District Court instructed the jury to consider invalidity. The jury returned its verdict less than two hours later. JA9388-90, 3428:23-3436:12.

The jury found that Defendants do not infringe claims 1, 2, 32, 35-37, 58, 65 and 66 of the '194 Patent and claims 1, 5, 6, 12, 15, 33, 37, 38, 45, 52 and 55 of the '962 Patent (the "Asserted Claims") (Websense was not accused of infringement of the '962 Patent). The jury further found invalid as anticipated and obvious claims 1, 2, 32, 35, 36, 37, 38, 58, 65 and 66 of the '194 Patent and claims 1, 5, 6, 12, 15, 21, 33, 37, 38, 45, 52 and 55 of the '962 Patent. JA1-2.

4. Sophos Admitted Infringement at Trial

During closing argument Sophos' counsel admitted infringement: "Finjan filed patents, and the Patent Office granted patents, and those patent claims cover what we do." JA8982, 3351:25-3352:2. Sophos also stated that it had not "contended for a minute in this case that our products are not covered by their patents." *Id.*, 3352:3-5. Rather than challenge infringement, Sophos instead argued that the Asserted Claims were invalid because they covered Sweep-InterCheck, a predecessor of Sophos' accused products.

The jury returned a verdict that Sophos does not infringe, despite Sophos' concession during trial that it infringed and the absence of any rebuttal to Finjan's detailed infringement proofs. JA5.

E. Post-Trial Motions

Finjan filed motions for JMOL against each defendant after the close of Defendants' case in chief arguing, *inter alia*, that no reasonable jury could find the Asserted Claims invalid. JA257. Finjan renewed its motions at the end of the close of evidence. JA258. After the jury verdict, Finjan filed renewed motions for JMOL of validity and a motion for a new trial. JA261. The District Court denied each of Finjan's motions. JA110.

III. REPRESENTATIVE CLAIMS

Representative independent claims are reproduced below:

> ‘194 Patent Claim 1. A computer-based method, comprising the steps of
>
> receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client;
>
> comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be

> attempted by the Downloadable, against a security policy to determine if the security policy has been violated;
>
> and preventing execution of the Downloadable by the client if the security policy has been violated.

JA287.

> ‘962 Patent Claim 1. A computer-based method, comprising:
>
> monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;
>
> interrupting processing of the request; comparing information pertaining to the Downloadable against a predetermined security policy; and
>
> performing a predetermined responsive action based on the comparison.

JA306.

IV. SUMMARY OF THE ARGUMENT

Finjan respectfully requests that this Court find the Asserted Claims valid as a matter of law over the Asserted Prior Art. Defendants failed to present clear and convincing evidence that the Asserted Claims are invalid. While validity was hotly contested at trial, based on the facts that were not disputed, the Asserted Prior Art did not satisfy all of the limitations of the Asserted Claims when those claims are properly construed. For example, the prior art did not teach proactive, behavior-based analysis or monitoring a plurality of subsystems in real-time for suspicious operations.

In the alternative, Finjan seeks a new trial on validity on three grounds. *First*, the District Court committed significant and highly prejudicial error in excluding Finjan's validity expert from testifying during redirect examination regarding his review of machine executable code for the Asserted Prior Art. The District Court based this ruling on an incorrect finding that Finjan's expert had not previously provided testimony on this topic, when in fact he did during both direct and cross-examination. Defendants seized on this error, arguing as a primary theme during closing argument that Finjan's expert's analysis should not be credited because he was purportedly unfamiliar with the operation of the Asserted Prior Art because he did not review its source code. *Second*, a new trial on validity is necessary because of the facial inconsistency in the jury's verdict that (1) Sophos' current products do not infringe the Asserted Claims but (2) Sophos' earlier products anticipate the Asserted Claims. Sophos provided no basis for the jury to distinguish its prior art and accused products with respect to the Asserted Claims. *Third*, the verdict of invalidity of all Asserted Claims is against the clear weight of evidence.

V. ARGUMENT

A. Standard of Review and Applicable Law

This Court reviews the denial of Finjan's motions for JMOL *de novo* under Third Circuit regional law. *Union Carbide Chems. & Plastics Tech. Corp. v. Shell Oil Co.*, 425 F.3d 1366, 1372 (Fed. Cir. 2005); *Eddy v. V.I. Water & Power Auth.*, 369 F.3d 227, 230 (3d Cir. 2004). This Court considers without deference whether there is substantial evidence to support the jury verdicts of invalidity of the '194 and '962 Patents. *Id.*

Reversal of the District Court's denial of JMOL is appropriate "if the jury's factual findings are not supported by substantial evidence or if the legal conclusions implied from the jury's verdict cannot in law be supported by those findings." *ADC Telecomms., Inc. v. Switchcraft, Inc.*, 281 F. App'x 989, 991 (Fed. Cir. 2008).

Claim construction is an issue of law that this Court reviews *de novo*. *Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1451 (Fed. Cir. 1998) (en banc).

Applying Third Circuit law, the denial of Finjan's motion for a new trial is reviewed under an abuse of discretion standard, except where the District Court based its denial on an application of law, in which case this Court's review is plenary. *McKenna v. City of Phila.*, 582 F.3d 447, 460 (3d Cir. 2009).

A new trial is warranted where (1) the jury's verdict is against the clear weight of evidence, and a new trial must be granted to prevent a miscarriage of justice; (2) the jury's verdict was facially inconsistent; (3) substantial errors were made in the admission or rejection of evidence or the giving or refusal of jury instructions; or (4) improper conduct by an attorney or the court unfairly influenced the verdict. *See Norman v. Elkin*, 849 F. Supp. 2d 418, 422 (D. Del. 2012).

When presented with a motion for a new trial, the court "does not view the evidence in the light most favorable to the verdict winner, but instead exercises its own judgment in assessing the evidence." *Marra v. Phila. Housing Auth.*, 497 F.3d 286, 309 n.18 (3d Cir. 2007).

Under the law of the Third Circuit, this Court reviews the District Court's decision to exclude or admit evidence for an abuse of discretion. *Primus v. Target Corp.*, No. 12-3894, 2013 WL 4019830, at *1 (3d Cir. Aug. 8, 2013). An evidentiary ruling is reversible when it affects a party's substantive rights. *Hirst v. Inverness Hotel Corp.*, 544 F.3d 221, 228 (3d Cir. 2008).

B. Defendants Failed to Establish with Clear and Convincing Evidence that the '194 Patent is Invalid

The District Court erred in denying Finjan's motion for JMOL that the Asserted Claims of the '194 Patent are valid. At trial, Defendants argued that the Asserted Claims were rendered obvious by a proposed combination of

ThunderByte 7.0 and MIMESweeper and anticipated by a purported combination of Sophos' Sweep and InterCheck products. As shown below, JMOL of validity was warranted because Defendants failed to provide clear and convincing evidence of invalidity on either ground. The Asserted Prior Art was limited to signature-based detection and does not teach the claimed proactive, behavioral-based identification of threats that was central to the '194 Patent.

1. The Asserted Claims of the '194 Patent are Not Obvious Over ThunderByte 7.0 in Combination With MIMESweeper

Defendants did not provide the jury with clear and convincing evidence that the Asserted Claims of the '194 Patent are obvious over the combination of ThunderByte 7.0 and MIMESweeper. There was no evidence that ThunderByte 7.0 could have been combined with MIMESweeper in the specific manner Defendants suggested. Moreover, even if possible, the proposed combination would not have practiced the limitations of the Asserted Claims. Tellingly, the Asserted Claims issued over ThunderByte, which was considered by the Patent Office during prosecution of the '194 Patent, confirming the validity of these claims. JA26232; JA26361.

a. Defendants Failed to Show that a Person of Ordinary Skill in the Art Could Have Combined ThunderByte 7.0 With MIMESweeper

Defendants' entire obviousness case for the '194 Patent is premised on a specific combination of the heuristic scanning functionality of ThunderByte 7.0 with the gateway functionality of MIMESweeper, yet Defendants failed to establish that such a combination was possible, let alone that a person of ordinary skill in the art would have been motivated to do so. *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1360 (Fed. Cir. 2012) (proponent of invalidity bears burden of showing "reasonable expectation of success in" proposed combination). For this reason, all of the Asserted Claims of the '194 Patent are valid over ThunderByte and MIMESweeper.

As their only evidence that the proposed combination was even possible, Defendants relied on two nontechnical articles stating that MIMESweeper could be used with ThunderByte, by using ThunderByte *to scan email attachments*. JA14749-50; JA14831-32. To yield the claimed inventions, however, it would have been necessary to combine ThunderByte's heuristic scanning (i.e., a series of commands that result in a user either accepting or denying the scanned file) with MIMESweeper's gateway functionality (i.e., an email gateway designed to process and send email as quickly as possible). The articles do not discuss or even suggest that ThunderByte and MIMESweeper could be combined in this fashion. JA8867-68, 3061:15-3062:8, 3065:21-3066:5. Defendants' expert did not testify that he or anyone else had ever successfully combined ThunderByte with MIMESweeper. *See* JA8005-08, 2131:23-2143:17.

Beyond Defendants' failure to carry their burden to show that the proposed ThunderByte/MIMESweeper combination was possible, Finjan offered unrebutted affirmative evidence that the proposed construction was *not* possible. Finjan's expert conducted experiments proving that ThunderByte 7.0 was incompatible with the Windows NT system used by MIMESweeper. JA8867, 3059:23-3062:8; JA8869, 3069:1-11. The expert's technical explanation of why this combination was impossible—because the MS DOS system would be constantly triggering manual acknowledgements—was not challenged at trial during cross-examination or otherwise. Specifically, a combination of ThunderByte and MIMESweeper would require a series of commands to be executed on every single email that would require a user to click either accept or deny, resulting in a user manually scanning every email that was sent through the gateway. Such a system would be unworkable because the number of emails that would actually be processed through the system would be slowed to a crawl. *Id.*

Because Defendants failed to provide clear and convincing evidence that the heuristic scanning functionality of Version 7.0 of ThunderByte could be combined with MIMESweeper (and undisputed record evidence showed that it could *not* be so combined), there was no basis to find the Asserted Claims of the '194 Patent obvious, and the District Courts' denial of JMOL of validity was reversible error.

b. ThunderByte in Combination With MIMESweeper Does Not Disclose All of the Limitations of the Asserted Claims of the '194 Patent

Beyond the lack of evidence that ThunderByte could have been combined as proposed with MIMESweeper, JMOL of validity was further warranted because ThunderByte and MIMESweeper do not disclose all the limitations of the Asserted Claims of the '194 Patent, as properly construed.

(i) ThunderByte Did Not Disclose Use of "Security Profile Data" Including a "List of Suspicious Computer Operations"

A key innovation of the '194 Patent over the prior art is the identification of threats by examining behaviors of Downloadables, as opposed to just searching for strings of code that are known to correspond to malware. This focus on behaviors allows for the identification of unknown threats, which was not possible with the prior art signature-based systems. Consistent with this approach, the Asserted Claims recite examining "security profile data pertaining to a Downloadable" that includes "a list of suspicious computer ***operations***," in order to identify potentially harmful Downloadables. JA287, 10:8-18 (emphasis added).

Thus, to invalidate the Asserted Claims, prior art must actually examine the operations that the Downloadable would attempt to perform. ThunderByte does not do so because it only looks to match known text strings and file attributes that correspond to known malicious software without actually analyzing the operations of the Downloadables it is inspecting (an undisputed fact). JA8867-69, 3062:9-3067:8. Therefore, given how the claims were construed, ThunderByte cannot invalidate the Asserted Claims.

In denying JMOL of validity, the District Court cited testimony from Defendants' expert that the ThunderByte user manual discusses disassembling files to identify suspicious instruction sequences. JA29. Yet, it is only files' characteristics that are analyzed, not the actual operations of the files, as claimed. JA8867-68, 3062:24-3065:6. Indeed, analyzing a file's characteristics is akin to signature matching because a sequence of the file's bytes is matched against a signature database. The '194 Patent, on the other hand, requires a more robust analysis of the actual operations of the file, and may flag a Downloadable as malicious even if the sequence of bytes does not match a preexisting database. Moreover, Defendants did not, and cannot, show that ThunderByte generates a *list* of suspicious computer *operations* because the disassembling of files does not result in a list at all, and refers instead to the raw components of that file rather than a list of what that file intends to do. *Id.* Thus, ThunderByte cannot render obvious any of the Asserted Claims of the '194 Patent.

(ii) ThunderByte Did Not Process JavaScript or Visual Basic

Another important inventive concept of the '194 Patent is the realization that script-based languages for execution by an Internet browser, such as JavaScript and Visual Basic, could pose a significant security threat. Previously, programs were installed on a computer using traditional file management methods and Internet browsers provided static content. The advent of JavaScript and similar script languages (such as ActiveX) allowed Internet browsers to quickly download and execute code without first installing it on a computer. JA7029, 504:3-505:23. While these advances allowed the functionality of the Internet-based experience to improve, they also created a new security risk in that traditional security software was not designed to protect against threats from such Downloadable code. *Id.*, 505:24-506:9.

As of 1996, it was nearly impossible to defend against JavaScript and ActiveX attacks because the programs could run independently and destroy a computer by themselves, unlike traditional parasitic viruses which would merely attach themselves to other files and slowly cause a computer to run out of memory. As these languages were Internet-based, the problem was escalated because malware could spread quickly, crashing entire networks of computers in one fell swoop.

There was thus a critical need for the capability to stop a program based on the *actions* it performed (such as a JavaScript that attempts to delete the files on a hard drive), rather than just passively scanning the bytes of the files on the hard drive to see if any viruses had attached themselves (as traditional anti-virus programs did). Finjan's new technologies addressed this need, especially regarding JavaScript and Visual Basic, by deducing the operations of the file, i.e. the actions it would perform, before the file could execute. The '194 Patent solves an important deficiency in the prior art by providing for the scanning of Internet applets, such as JavaScript programs downloaded by an Internet browser. JA283, 1:37-57. At the time, this was a complete departure from traditional anti-virus programs, which were only equipped to analyze traditional languages. Indeed, as previously noted, Finjan's name was selected to reflect the importance of containing threats posed by JavaScript. JA7030, 510:20-511:8.

Defendants failed to show that ThunderByte (alone or in combination with MIMESweeper) was capable of detecting suspicious operations in JavaScript or Visual Basic script code within a Downloadable, as recited in Claims 10, 11, 33, 35 and 36 of the '194 Patent. JA8869, 3069:12-21. To the contrary, Defendants' expert conceded that ThunderByte did not mention JavaScript or Visual Basic script, and he only theorized that it would have been obvious to modify ThunderByte to process such files. JA8012, 2160:5-2161:19; JA8020, 2193:2-11.

Defendants did not present substantial evidence of obviousness. Defendants' expert did not identify any prior art reference with which ThunderByte and MIMESweeper could be combined to yield this result. At most, he provided conclusory testimony that JavaScript and Visual Basic were known before the claimed invention, that ThunderByte contemplated scanning files in different languages and that there was a general concept that it was helpful to have "defense in depth," i.e., as much defense as possible. JA30. This is nothing more than a hindsight recognition that it would have been helpful to scan JavaScript and Visual Basic for malware. But, as explained above, the unique characteristics of those Internet-based languages required a fundamentally new type of anti-virus technology, and the ability to detect threats in such languages based on behavioral analysis was a key component of the inventions of the '194 Patent. *See, e.g.*, JA283, 1:29-57. Moreover, Defendants' expert did not explain how ThunderByte could be modified to search for suspicious operations in Internet applets written in Visual Basic and JavaScript code.

The conclusory *ipse dixit* analysis of Defendants' expert that it would have been obvious to monitor JavaScript code and similar files—even though no one had thought to do so before Finjan founded a company to implement this idea—"cannot be enough to constitute clear and convincing evidence" of an obviousness case. *Cephalon, Inc. v. Watson Pharms., Inc.*, 707 F.3d 1330, 1338 (Fed. Cir. 2013) (*ipse dixit* statements by expert insufficient to sustain invalidity case).

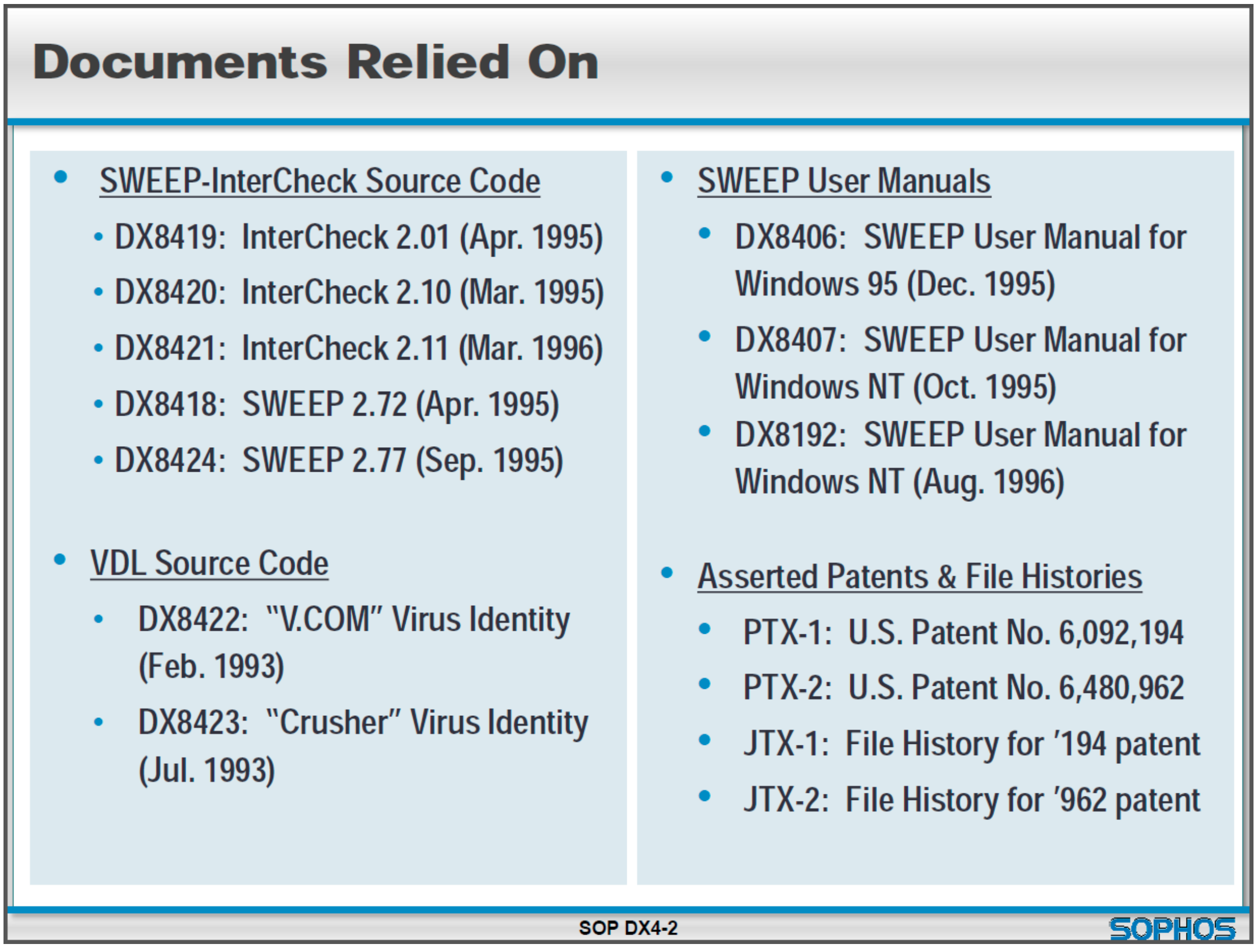
Defendants failed to explain how this novel concept would have been obvious to a person of ordinary skill in the art at the time of the alleged invention, given the focus of the prior art on file systems, and thereby did not establish a *prima facie* case of obviousness. *TriMed, Inc. v. Stryker Corp.*, 608 F.3d 1333, 1342-43 (Fed. Cir. 2010) (reversing summary judgment of invalidity: "[m]erely saying that an invention is a logical, commonsense solution to a known problem does not make it so."); *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 417, 421 (2007) ("A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post reasoning") (citations omitted). For these reasons, no reasonable jury could have found obvious claims 10, 11, 33, 35 and 36.

2. The Asserted Claims of the '194 Patent are Not Anticipated By Sweep and InterCheck

Defendants' anticipation case for the '194 Patent rested exclusively on their fundamentally flawed proposed combination of Sweep and InterCheck. Defendants relied on an improper combination of multiple versions of source code that did not correspond to the asserted prior art. Moreover, Defendants did not introduce clear and convincing evidence that the purported Sweep-InterCheck combination would have practiced all of the limitations of the Asserted Claims of the '194 Patent. As shown below, there is little actual dispute as to the operation of Sweep-InterCheck with respect to the claim limitations at issue. Instead, Finjan contends that the undisputed operations of Sweep-InterCheck do not satisfy the claim limitations, as properly construed. Defendants' invalidity arguments fail as a matter of law, and JMOL of validity is warranted on each of these independent grounds.

(i) Defendants Improperly Argued Anticipation Based on Multiple Versions of Source Code Not Tied to the Asserted Prior Art

Defendants' Sweep-InterCheck argument fails, as a matter of law, because Defendants improperly argued anticipation based on a combination of various Sweep-InterCheck source code and software versions and manuals, as shown in Defendants' trial demonstrative reproduced below.



Documents Relied On

- SWEEP-InterCheck Source Code
  - DX8419: InterCheck 2.01 (Apr. 1995)
  - DX8420: InterCheck 2.10 (Mar. 1995)
  - DX8421: InterCheck 2.11 (Mar. 1996)
  - DX8418: SWEEP 2.72 (Apr. 1995)
  - DX8424: SWEEP 2.77 (Sep. 1995)
- VDL Source Code
  - DX8422: "V.COM" Virus Identity (Feb. 1993)
  - DX8423: "Crusher" Virus Identity (Jul. 1993)
- SWEEP User Manuals
  - DX8406: SWEEP User Manual for Windows 95 (Dec. 1995)
  - DX8407: SWEEP User Manual for Windows NT (Oct. 1995)
  - DX8192: SWEEP User Manual for Windows NT (Aug. 1996)
- Asserted Patents & File Histories
  - PTX-1: U.S. Patent No. 6,092,194
  - PTX-2: U.S. Patent No. 6,480,962
  - JTX-1: File History for '194 patent
  - JTX-2: File History for '962 patent

SOP DX4-2

SOPHOS

These separate materials—most of which did not correspond to version 2.72 Sweep and version 2.11 of InterCheck, the only versions asserted at trial—do not constitute a single prior art reference and, thus, cannot support an anticipation defense. *See Kyocera Wireless Corp. v. ITC*, 545 F.3d 1340, 1351-52 (Fed. Cir. 2008) (collection of technical specifications collectively known as the GSM standard do not function as a single prior art reference); *Dayco Prods., Inc. v. Total Containment, Inc.*, 329 F.3d 1358, 1368-69 (Fed. Cir. 2003) (anticipation requires that every element of a claim must be found in a single reference).

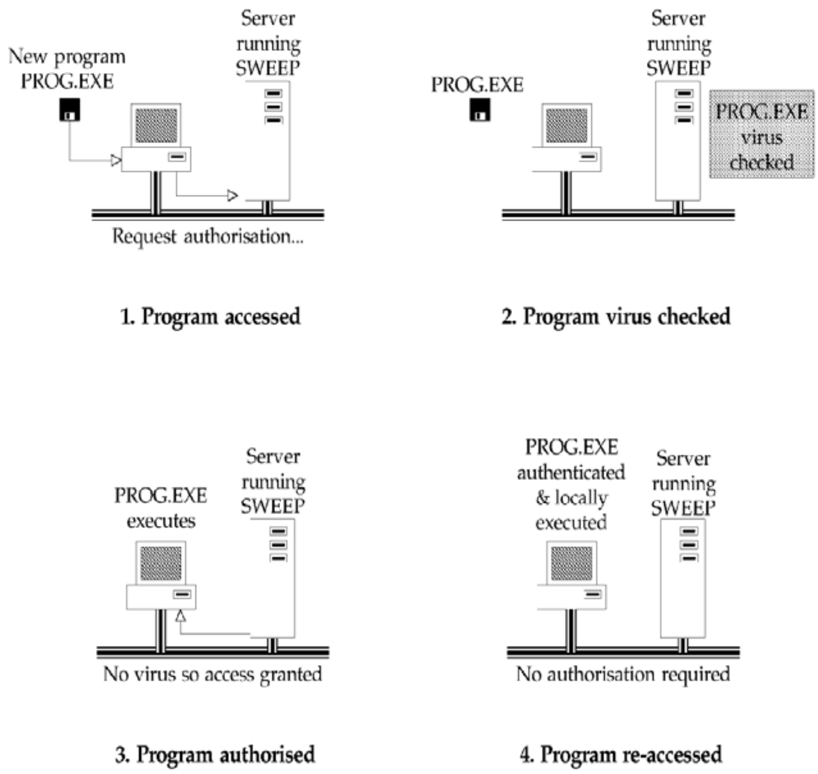
(ii) Sweep-InterCheck Did Not Check Downloadables With a Server that "Serves as a Gateway to the Client"

Sweep-InterCheck did not disclose a server that "serves as a *gateway* to a client." Specifically, the Asserted Claims of the '194 Patent state that the Downloadable is received *from* the gateway server by the client, requiring that the server checks incoming Downloadable files before they are delivered to the client. In contrast to the prior art's focus on periodically scanning files after they are downloaded to a local computer, the '194 Patent taught using a gateway to inspect files before they are downloaded (for example, from the Internet) to the local computer.

As Finjan's expert explained, Sweep-InterCheck did not have such a gateway. JA8891, 3156:9-3157:7. The pertinent facts were not disputed by the parties, and the District Court's denial of JMOL was premised on a legally incorrect claim construction—that Sweep-InterCheck can satisfy this limitation by examining files *after* they have already been downloaded to the client.[1]

[1] Defendants did not dispute the dispositive fact that Sweep only checks files after they have been downloaded to the client. Defendants' expert conceded that files are loaded directly onto the client (either through a floppy disk drive or the Internet) *without being examined*, i.e., that there is no gateway. JA8182, 2494:23-2495:6 ("Q: The server gets a copy of it, but the client receives it first, Correct? A: The client receives it first, right."); JA8113-14, 2395:18-2400:2 (Downloadable can be downloaded from Internet onto client computer without being scanned by Sweep server).

Specifically, as illustrated below, in contrast to the claimed gateway server in the ‘194 Patent, potentially malicious files are not examined by Sweep-InterCheck until they are first delivered to the client and then executed. Upon execution, if the file is not recognized, the client asks the server (running Sweep) to evaluate a copy of that file (shown as Step 1 below). At Step 2, the Sweep server inspects the Downloadable. In Step 3, based on the server’s response, the client will decide to execute or delete the file in question. JA8890, 3153:18-3154:6 (“The server does not prevent the client from doing anything. The server scans the file and returns a verdict. It's up to the client to decide what to do with that particular file.”). Step 4 shows the case where the Downloadable has already been inspected by the Sweep server, in which case it is executed without further inspection. Thus, no server acts as a gateway by blocking a harmful Downloadable from being *downloaded* onto the client, as required by the Asserted Claims.



1. Program accessed

2. Program virus checked

3. Program authorised

4. Program re-accessed

22

SOP-0549466

DX8192-0022

JA18726.

As a matter of claim construction, examining files after they have already been downloaded to the client means that the server is not a "gateway" to the client. While the District Court did not construe the term "gateway," the specification makes clear that the gateway acts to inspect potentially malicious software before it is downloaded, and only forwards the Downloadable to the client after it has been inspected. *See, e.g.*, JA284, 3:9-13 ("The internal network security system 110 examines Downloadables received from external computer network 105, ***and prevents Downloadables deemed suspicious from reaching the internal computer network***.") (emphasis added).

The District Court erred in denying JMOL of validity because the "gateway" must check the Downloadable before it is downloaded to the client, and it is undisputed that Sweep does not do this. Therefore, Sweep-InterCheck cannot anticipate any of the Asserted Claims.

(iii) Sweep-InterCheck Did Not Use a "Security Policy" Based on Operations

Sweep-InterCheck does not satisfy the limitation in all Asserted Claims of the '194 Patent that "the Downloadable security profile data includes a list a suspicious computer *operations* that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated." JA8872, 3079:14-3080:21. As previously noted, the ability to identify threats through proactive behavioral analysis, including previously unknown threats, was a key feature of the '194 Patent.

This limitation requires analysis of "operations." *Id.* While the term "operations" was not construed, the specification provides that operations are actions carried out by the Downloadable, and provides a list of examples of potentially suspicious operatives, such as reading or writing to certain files, modifying the registry or, starting new processes. JA285, 5:59-6:4. Accordingly, "operations" cannot be satisfied simply by matching text strings in the code without looking at the actions those strings would cause. *C.f. Datascape, Inc. v. Sprint Spectrum, L.P.*, No. 1:09-cv-00136, Special Master Report & Recommendation on Claim Construction (N.D. Ga. Nov. 30, 2011), ECF No. 71-1 at 27 (special master: construing "operation" as "a specific action or sequence of actions to be carried out").

The dispute over this limitation reduces to a question of claim construction. As the Asserted Claims, when properly construed, require a comparison of behavior to a policy, not just matching code against a known list of malicious code, there was no evidence presented to the jury that Sweep-InterCheck satisfied this limitation and JMOL of validity of all of the Asserted Claims was warranted. Instead of checking operations to identify malicious software, Sweep-InterCheck is limited to providing traditional fingerprint/signature matching based detection, i.e., matching code text to known malicious text. JA8872, 3079:14-3080:21. Sweep-InterCheck does not perform an actual analysis of the Downloadable's actions. *Id.*

Defendants' only response in opposing JMOL, that Sweep-InterCheck satisfies the "operations" limitation because it was capable of detecting "unknown malware, such as polymorphic viruses" (JA14009) is contrary to the very testimony cited by Sophos.[2] That testimony confirms that Sweep-InterCheck detects such polymorphic viruses simply by looking for *known* signatures of code, not by performing the claimed analysis of operations to detect unknown malicious code. *See* JA8101-02, 2349:5-2351:5 (detecting polymorphic virus by looking for known patterns in code).

For example, the testimony relied upon by the District Court (JA49) as purportedly showing that Sweep-InterCheck was capable of detecting unknown viruses (supposedly by looking at behaviors), actually shows simply matching text strings in the code against a list of predefined known text sequences:

> Q. And is decryption a suspicious operation?
>
> A. Highly suspicious operation, yes.
>
> Q. And so, how did this detect that suspicious operation?
>
> A. So, the execution starts here. It matches byte E8, then byte C1, and then byte FF, and so on. It then loads the rest of the virus. It then looks in the first seven bytes of the rest. It looks for this random sequence. So you can have a sequence of 9C, 50, 51, so on, in any order. That is the polymorphic bit of the virus.
>
> It then looks for another A bytes, another bytes for another random sequence, and so on.

JA49 citing JA8102, 2350:3-13.

[2] A "polymorphic" virus is able to change its code, making it more difficult to identify with basic signature detection technology. JA7041, 554:19-555:8.

As shown from this testimony, the Sweep-InterCheck product is matching a series of bytes in an incoming file to those in a preexisting database. The ‘194 Patent, on the other hand, requires more—a determination of the actual operations of the incoming file.

Therefore no reasonable jury could have found that Sweep-InterCheck invalidates the Asserted Claims.

(iv) Sweep-InterCheck Did Not Process JavaScript or Visual Basic Script Downloadables

Sweep-InterCheck cannot invalidate claims 10, 11, 33, 35 and 36 of the ‘194 Patent, which recite evaluating Downloadables where the “Downloadable includes” either JavaScript or Visual Basic code. JA287-88; JA8125, 2443:12-2444:15. It was undisputed that Sweep-InterCheck was not capable of examining such code in a Downloadable for malware, as claimed. JA8183, 2499:4-15 (“Q. The JavaScript is not actually checked for a virus. Correct? A. [Defendants’ expert:] It's not.”); JA8875, 3093:4-6. As previously discussed, monitoring JavaScript and Visual Basic script for malicious behavior was an important improvement over the prior art.

In denying JMOL, the District Court accepted Defendants’ incorrect claim construction argument that the claims do not require that the JavaScript or Visual Basic script be checked for malware. The ‘194 Patent makes clear that JavaScript and similar type code are included in the security scan. *See, e.g.*, JA284, 4:41-61. Indeed, the ‘194 Patent explains that one of its primary improvements over the prior art is the ability to inspect Internet browser Downloadables, such as JavaScript and Visual Basic applets. JA283, 1:37-57. Furthermore, a plain reading of the claims provides that the Downloadable security profile data must pertain to the Downloadable and contain a list of operations within that Downloadable. The dependent claims require the Downloadable to be JavaScript or Visual Basic script. Thus, the operations of the JavaScript and the Visual Basic script must be deduced and compared to a security policy to determine whether they should be executed.

Accordingly, it was erroneous for the District Court to conclude that these claims could be invalidated by prior art that was not capable of inspecting JavaScript or Visual Basic code and, as a matter of law, Sweep-InterCheck cannot invalidate claims 10, 11, 33, 35 and 36 of the ‘194 Patent.

C. Defendants Failed to Establish With Clear and Convincing Evidence that the ‘962 Patent is Invalid

The District Court erred in denying Finjan’s motion for JMOL that the Asserted Claims of the ‘962 Patent are valid. At trial, Defendants argued that the Asserted Claims were anticipated by (1) a purported combination of Sophos’ Sweep and InterCheck products and (2) NAV 95. Defendants did not provide any obviousness analysis to the jury for the ‘962 Patent (other than with respect to a proposed combination of NAV 95 and HotJava for a single claim). As shown below, Defendants did not provide clear and convincing evidence of invalidity on either ground.

1. The Asserted Claims of the ‘962 Patent are Not Anticipated By Sweep and InterCheck

As previously demonstrated, Defendants improperly argued anticipation based on multiple versions of source code for Sweep and InterCheck, many of which did not correspond to the version 2.72 of Sweep and version 2.11 of InterCheck actually asserted as prior art. Moreover, Defendants failed to establish that the proposed Sweep-InterCheck combination disclosed all of the limitations of the Asserted Claims of the ‘962 Patent.

a. Sweep-InterCheck Did Not Monitor Files “During Runtime”

While the prior art was focused on periodically inspecting files already downloaded to a local computer, the ‘962 Patent taught inspecting files “during runtime.” As acknowledged by Defendants’ expert, “[d]uring runtime means during the execution of the program.” JA8127, 2453:18-22. This is advantageous because it provides an additional layer of protection that is necessary to protect against Internet-based malware. For example, according to the prior art, if a file is scanned before execution and there is no corresponding fingerprint in the database, the file will be allowed to run without any further analysis. The ‘962 Patent, on the other hand, will continue to monitor the file for malicious operations.

As such, if a malicious operation is attempted, the ‘962 Patent will stop the action, even if the program was initially deemed benign.

Sweep-InterCheck cannot invalidate the Asserted Claims because it did not monitor files “during runtime,” as recited in all of the Asserted Claims. JA8876, 3095:12-3096:20. With Sweep-InterCheck, before a program is executed, the code is sent to the server for analysis—a *pre*-runtime check to determine if it is safe. After the file is approved there is no “runtime” analysis while the file is actually being executed. *Id*.

Defendants argued that the “during runtime” limitation is satisfied when Sweep-InterCheck intercepts actions, such as opening, closing or writing a file, but these are all actions that take place *before* or *after* a program is executed, not while the program is running. JA8127-28, 2453:17-2454:18. Sweep-InterCheck does not perform any analysis of the file or its operations after the file is actually running. In contrast, the ‘962 Patent requires the operating system to be consistently monitored so that if a file that is originally determined to be safe later performs a malicious operation in runtime, that operation will be stopped to prevent harm to the system. *Id.* Thus, for this reason alone, Sweep-InterCheck cannot anticipate any of the Asserted Claims of the ‘962 Patent as a matter of law.

b. Sweep-InterCheck Did Not Compare Information "Pertaining to the Downloadable," and Does Not Have a "Comparator" or a "Response Engine"

Finjan demonstrated that Sweep-InterCheck did not perform the step of "comparing information pertaining to the Downloadable against a predetermined security policy." JA8876, 3096:21-3097:11. The claims of the '962 Patent require that a Downloadable make a request, the request be interrupted and that information pertaining to that Downloadable be compared with a security policy. *Id.* Sweep-InterCheck, on the other hand, only looks at information about the *target* of a Downloadable's request (but not at information about the Downloadable itself). For example, if a request is made to open a file, Sweep-InterCheck will only determine whether the particular file that is being opened should be allowed to proceed. However, this does not disclose the required claim element of comparing information pertaining to the *Downloadable* because the '962 Patent requires not only looking at the file being opened, but also looking at the file that made the original request to open the file.

This distinction is important because it provides an additional layer of protection for the system. For example, if a simple request to open a file is generally allowed, then a program could open up all of the files on a computer and crash the system. However, with the '962 Patent, the source of the open file request is analyzed. Therefore, the '962 Patent would protect against the crash because it would recognize that the same program tried to open multiple files and stop the program from opening any further files. JA8876-77, 3096:21-3097:11, 3099:12-22.

Defendants' expert simply testified that Sweep-InterCheck performs an action if a virus is detected, but did not disclose how that virus is detected. *See* JA8128-29, 2456:14-2458:3. Because Sweep-InterCheck never compares information pertaining to the Downloadable in determining a responsive action, the '962 Patent is valid over Sweep-InterCheck.

2. The Asserted Claims of the '962 Patent are Not Anticipated By Norton Antivirus 95

Defendants also asserted anticipation of the Asserted Claims of the '962 Patent based on NAV 95. No reasonable jury could have found in favor of Defendants and JMOL of validity was warranted because of the absence of clear and convincing evidence that NAV 95 disclosed various limitations of the Asserted Claims, each of which is an independent basis to find validity.

(i) NAV 95 Did Not Monitor a "Plurality of Subsystems"

NAV 95 cannot invalidate any of the Asserted Claims of the '962 Patent because it did not monitor "a plurality of subsystems" of an operating system. JA306, 7:11-12. A significant advance of the '962 Patent was the ability to monitor multiple subsystems at the same time, including the file management system, network management system, process system and memory system. *Id.*, 4:19-31.

When NAV 95 was introduced, viruses were generally known only to infect files. It is thus unsurprising that NAV 95—like other prior art—was focused on protecting file systems, and did not monitor multiple subsystems, and especially network management systems. The prior art did not recognize that malware could pose a concern to other subsystems of the operating system, such as networks systems. JA8861-63, 3036:14-3037:7, 3038:6-3043:4; JA8881-82, 3118:20-3120:4.

In denying JMOL, the District Court relied upon the testimony of Defendants' expert that NAV 95 satisfied this limitation by purportedly monitoring two subsystems: (1) input/output operations and (2) file system operations. JA7797-98, 2101:17-2102:2. Finjan, however, provided unrebutted testimony that the "input/output" monitoring of NAV 95 is limited to "disk space operations [e.g., to] format the hard drive, modify file, modify an attribute of an executable file," all of which are operations of the *file system*—not a distinct subsystem of the operating system. JA8858, 3025:4-12; JA8861, 3036:14-3037:7; JA8862-63, 3040:15-3043:4.[3]

[3] The District Court noted that a NAV 95 user manual and source code, a Microsoft book and Dr. Vigna's lecture notes refer to both file systems and input/output systems as supporting the Defendants' position that file systems are distinct

The specification of the '962 Patent confirms that the operations identified by Defendants' expert are file system operations, not the operations of a distinct subsystem. Specifically, the '962 Patent identifies four subsystems: file management, network management, process, and memory. JA304, 4:19-31. The '962 Patent does not identify "input/output" as a distinct subsystem (nor would it because these are file operations). Accordingly, as a matter of claim construction, Defendants did not identify any evidence that NAV 95 was capable of monitoring more than one subsystem for the simple reason that non-file based threats were not recognized in the prior art. For this reason alone, NAV 95 cannot invalidate any of the Asserted Claims of the '962 Patent.

(ii) NAV 95 Did Not Compare "Information Pertaining to a Downloadable Against a Predetermined Security Policy" and Does Not Perform a "Predetermined Responsive Action Based on the Comparison"

NAV 95 did not disclose the step of "comparing information pertaining to the Downloadable against a predetermined security policy," as recited in each of the Asserted Claims of the '962 Patent. JA8859, 3027:21-3029:4; JA8861, 3036:18-3038:5; JA8863, 3043:5-3045:13. NAV 95 only acts by blocking specific actions, but does not look to information about the source of the

subsystems from input/output systems. However, this supposed distinction between file and input/output systems is not relevant as Defendants did not identify any operations actually monitored by NAV 95 that are *not* operations of the file system. JA36.

action and does not compare information specifically pertaining to the Downloadable, as claimed. *Id.* Certain tasks would be blocked by NAV 95 no matter the Downloadable or corresponding information.

The District Court erred in relying on Defendants' testimony that this limitation is satisfied when NAV 95 (1) examines a request made by a Downloadable or (2) compares the identity of a program making a request against an exclusion list. JA37. Neither action satisfies the requirement of comparing information about the Downloadable in question.

With respect to NAV 95's examination of a Downloadable's request, the "Auto-Protect Advanced Settings" feature of NAV 95 allowed users to set NAV 95 to block or prompt a user before allowing five specific activities to take place (e.g., a low-level format of the hard disk or writing to hard disk boot sectors). JA8000, 2110:7-2111:11. These rules simply blocked certain actions, *regardless* of the source performing the action. The claims, however, require a comparison to a security policy of information that "pertain[s] to the Downloadable," not just blocking certain actions. JA8859, 3027:21-3029:4. Indeed, Websense's non-infringement expert agreed with this construction, testifying that the security profile information must "pertain[] to the specific downloadable. . . . it's extracted from the downloadable. So it's information that comes right out of that downloadable." JA8314, 2867:13-19; *see also* JA8325, 2910:21-2911:4 ("it's not something from somewhere else. It's actually from that particular downloadable"). NAV 95 did not process any such information about the Downloadable in applying these rules. JA8863, 3043:5-3045:13.

Defendants' expert also noted that NAV 95 could *exclude* certain directories or files from being scanned. JA8000, 2111:12-2112:18. But this is nothing more than *avoiding* examining certain files, and does not constitute comparing the substantive information "pertaining" to the files to some security policy. JA8861, 3037:16-24.

Thus, there was no factual dispute with respect to this limitation, only a legal claim construction question—if blindly blocking certain actions can satisfy the "information pertaining to the Downloadable" limitation. Finjan submits that, as a matter of law, it cannot, and JMOL of validity of all of the Asserted Claims over NAV 95 was warranted.

(iii) A Person of Ordinary Skill in the Art Would Not Have Been Motivated to Combine NAV 95 and HotJava

Defendants relied on a combination of NAV 95 and HotJava to allege invalidity of Claim 52 of the '962 Patent, but failed to establish that a person of ordinary skill in the art would have been motivated to combine HotJava with NAV 95 in the hodge-podge fashion proposed by Defendants' expert. To the contrary, there would have been no motivation to combine the two programs because they are directed to different tasks. HotJava monitored Java applets run by an Internet web browser, while NAV 95 monitored file systems for a local computer. JA8865, 3051:22-3053:2.

As with Defendants' conclusory analysis of the purported obviousness of these claims with respect to ThunderByte (*see* Section V(B)(1)(a)), Defendants' expert relied only on the general desire for "defense in depth"—that "you would run extra programs, to make sure you were defended against everything."—a plain hindsight analysis. JA8006, 2136:1-3. Under Defendants' logic, it would have been obvious to combine every possible anti-malware technology and apply it to every aspect of computer and network operations. But that was not being done at the time of the alleged invention. As previously noted, the prior art was focused on monitoring file systems for malware threats and had not taught the idea of monitoring Internet-based threats from Downloadables, such as Java applets—the inventive concept of claim 52. Accordingly, no reasonable jury could have found claim 52 obvious over NAV 95 and HotJava.

(iv) NAV 95 Did Not Have a "Downloadables Database"

The dispute over claim 55 is limited to a matter of claim construction. NAV 95 maintained a simple text activity log file, but did not use a "database." Therefore, NAV 95 did not perform claim 55's step of "adding information pertaining to the Downloadable to a suspicious Downloadables ***database***.” JA8864-65, 3048:8-15, 3050:23-3051:21.

The District Court erred in accepting NAV 95’s text log file as satisfying this limitation. JA38-39. Indeed, the ‘962 Patent specifically distinguishes between a “database” and an “event log.” JA304, 4:50-5:2 (“the runtime event monitor 320 records the violation with the ***event log*** … The response engine 318 analyzes security policies 332 stored in the ***security database***…”) (emphasis added).

The plain and ordinary meaning of “Database”—a well-known concept in computer science—is an organized, readily searchable set of data, and not just a simple text file (as is undisputedly used in NAV 95). JA8864-65, 3048:8-15, 3050:23-3051:21. Consistent with Finjan’s position, courts have repeatedly construed “database” as more than just a text file. *See, e.g., Timeline Inc. v. ProClarity Corp.*, 2-05-cv-01013, 2006 U.S. Dist. LEXIS 44478, at *32 (W.D. Wash. June 29, 2006) (Database: “a collection of organized information accessible through computer software, distinguishable from a collection of information stored in a flat file form such as a spreadsheet”); *MySpace, Inc. v. Graphon Corp.*, 756 F. Supp. 2d 1218, 1232 (N.D. Cal. 2010), *aff’d*, 672 F.3d 1250 (Fed. Cir. 2012) (database: “a collection of data with a given structure that can be stored and retrieved.”); *CIVIX-DDI LLC v. Hotels.com GP LLC*, 1:05-cv-

06869, 2010 WL 4386475, at *1 (N.D. Ill. Oct. 25, 2010) ("a collection of related information organized for convenient access"); *Geomas (Int'l) Ltd. V. Idearc Media Servs. – West, Inc.*, 2-06-cv-00475, 2008 WL 4966933, at *6 (E.D. Tex. Nov. 20, 2008) ("a collection of information or data organized such that a computer program can quickly retrieve selected information or data").

No reasonable jury could have found that NAV 95's simple text log file satisfies the "database" limitation, as properly construed. Therefore, a finding that claim 55 is valid is warranted.

3. Defendants Did Not Present an Obviousness Argument For the Asserted Claims of the '962 Patent

The jury verdict of obviousness of the Asserted Claims of the '962 Patent was entirely unsupported by the record. Other than with respect to the combination of NAV 95 and HotJava for claim 52 (which is deficient for the reasons set forth in Section (V)(C)(2)(iii)), Defendants did not present any obviousness analysis for these claims, relying only on the testimony in support of anticipation. *See, e.g.*, JA8118, 2414:20-2415:24; JA8180-81, 2486:9-2489:6, 2491:19-24 (Defendants' invalidity expert on Sweep-InterCheck: "I didn't provide an obviousness argument."). For the reasons discussed above with respect to anticipation and for the additional failure to present a *prima facie* obviousness case for these claims, the jury did not have any reasonable basis to find the Asserted Claims obvious.

D. A New Trial on Validity is Necessary

The District Court erred in denying Finjan's motion for a new trial.

First, a new trial is necessary to correct the District Court's substantial error in excluding the testimony of Finjan's validity expert regarding his review of binary and assembly language code for the asserted prior art, which severely distorted the jury's consideration of validity, prejudicing Finjan and contributing to the jury's erroneous verdict.

Second, a new trial is necessary in view of the jury's facially inconsistent findings that (1) Sophos' current products do not infringe the Asserted Claims while (2) Sophos' earlier products invalidate the Asserted Claims. Sophos did not argue any distinctions between its prior art and current products, and instead argued that both fall within the scope of the Asserted Claims. To the extent the jury agreed, it should have either found the claims infringed but invalid or not infringed and valid. Moreover, the jury does not appear to have properly considered invalidity, having apparently deliberated on the issue for less than two hours and having found the Asserted Claims of the '962 Patent obvious even though Defendants only argued anticipation.

Third, to the extent this Court is not prepared to find that the Asserted Claims are valid as a matter of law, at the very least the jury's verdict that the '194 and ‘962 Patents are invalid is against the clear weight of the evidence and this case should be remanded for a new trial on validity.

1. A New Trial is Necessary Because Finjan’s Validity Expert Should Have Been Permitted to Testify Regarding His Review of Binary and Assembly Language Code

The District Court committed a significant error in precluding Finjan’s validity expert, Dr. Vigna, from testifying during his rebuttal presentation regarding his review of machine executable code for the Asserted Prior Art. This error seriously compromised Finjan’s validity rebuttal case by impacting the credibility of Finjan’s technical experts, leaving them open to Defendants’ inappropriate and unwarranted criticisms regarding the use of source code, which may have adversely impacted both the validity and infringement sides of the case. For these reasons, a new trial on validity is necessary, as the errors were so prejudicial that denial of a new trial would be “inconsistent with substantial justice.” *Mondzelewski v. Pathmark Stores, Inc.*, No. 96-359 MMS, 2000 WL 654137, at *20 (D. Del. Mar. 20, 2000) (quotation and citations omitted).

On direct examination, Dr. Vigna explained that he studied the machine code for the Asserted Prior Art to understand its operation. Dr. Vigna could not review Defendants’ confidential source code due to his competitive activities in the field, but he did not need to do so because the machine code provides an even more reliable picture of how the products operate. JA8859-60, 3030:3-3031:11; JA8887, 3140:9-14. After Defendants cross-examined Dr. Vigna to suggest that his analysis of the prior art was inadequate because it was based on a review of machine code and not source code, Finjan attempt to rehabilitate Dr. Vigna during redirect examination. The District Court excluded this testimony based on the incorrect view that Dr. Vigna had not testified about this topic during his direct examination, when in fact he had.

Specifically, during his direct examination on validity, Dr. Vigna testified that he looked at the executable binary and assembly code for the asserted prior art to understand "what functions are called and what is done by the program, without looking at any source code."[4] JA8859-60, 3030:3-3031:11. For example, Dr. Vigna explained how he studied this code to understand how NAV 95 operated:

> Q. Did you do anything to confirm that your understanding of how NAV 95 operates was correct, at least according to the source code?
>
> A. So I ran the program, so I saw how it operates, how it scans files. I looked at the assembly, of course, to understand what functions are called and what is done by the program, without looking at any source code.

[4] As Dr. Vigna explained, "binary code" refers to "sequences of ones and zeros" that are actually "loaded into memory and executed" by a computer. "Assembly code" is "the code that is being executed at the machine level" "presented in a way that is human-readable. So you can see, for example, if there is an instruction that jumps to a certain address, if a certain function is called." JA8859-60, 3030:3-3031:11.

Id., 3030:7-3031:11. Dr. Vigna also explained how binary code is instructive in determining how a product actually works because that code is the set of instructions that a computer actually follows (as opposed to source code, which is not executed by a computer and, instead, is used to generate assembly and binary code). *Id.*; JA8887, 3140:9-14 ("the very ultimate way to understand how the program works is to look at the binary code because the same source code can actually be compiled into different binary code, and therefore, the only real way to know what gets executed is to look into the binary code."). As Dr. Vigna's review of this code was included in his direct examination, it should not have been precluded during his redirect.

Defendants further opened the door to Dr. Vigna's precluded rebuttal testimony when they attacked the reliability of Dr. Vigna's review of the prior art during cross-examination. In response to that attack, Dr. Vigna explained to the jury that, because source code can be compiled in different ways to yield different program functionality, his review of assembly language and binary code was more helpful than a review of source code:

> Q. The source code is a very important set of instructions on how the program operates. Right?
>
> A. Right. But what I am saying is ***the very ultimate way to understand how the program works is to look at the binary code because the same source code can actually be compiled***

> ***into different binary code, and, therefore, the only real way to know what gets executed is to look into the binary code.***
>
> * * *
>
> Q. Okay. But ultimately, you couldn't look at the source code in order to determine whether or not the operating system was performing that operation?
>
> A. ***Actually, I can go to a lower level, which is using debuggers and disassemblers to look actually at how that binary code operates.***

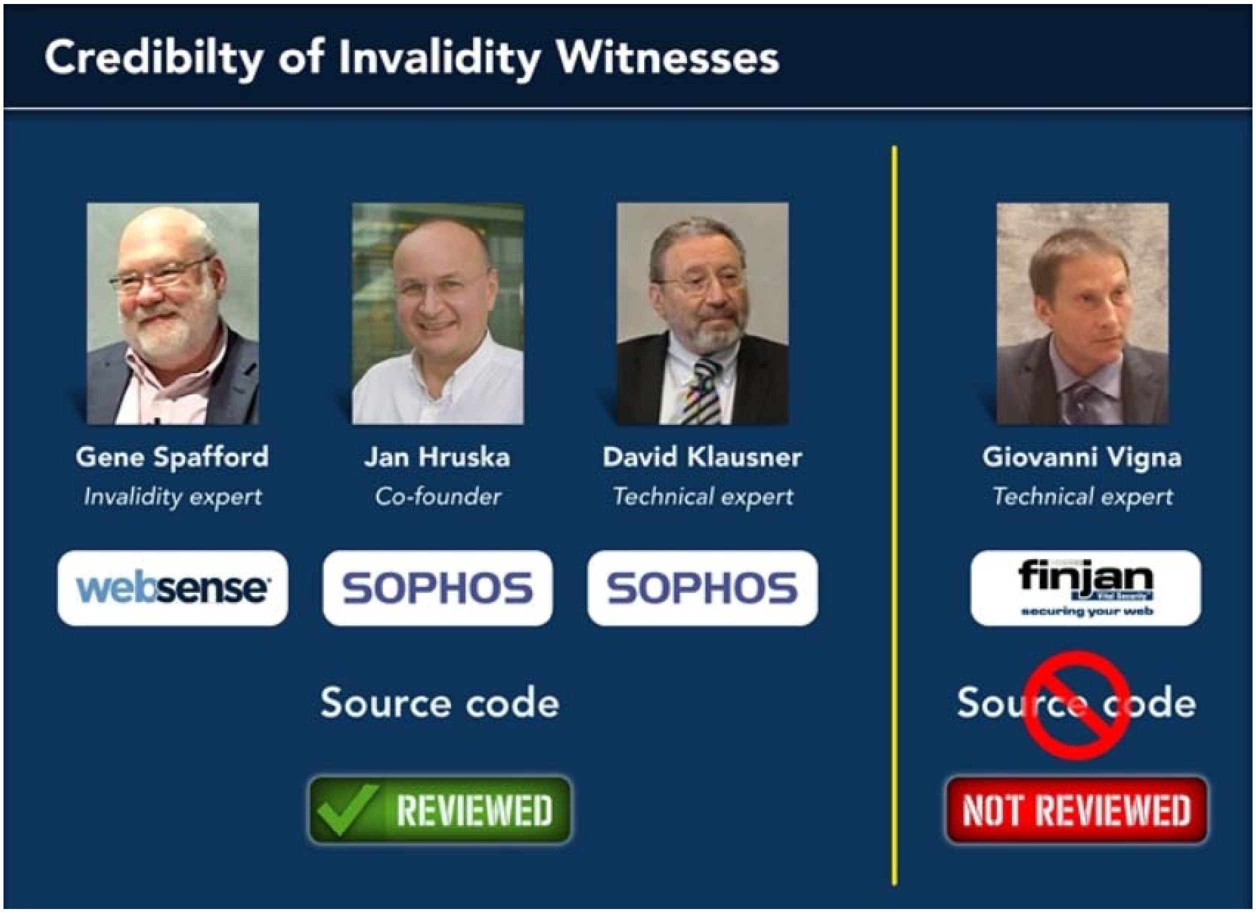
JA8887, 3140:7-14; JA8889, 3147:14-19 (emphasis added).

After the attempts by Defendants' counsel during cross-examination to discredit and admonish Dr. Vigna for not reviewing the source code, Finjan began to rehabilitate Dr. Vigna by asking him to explain why the binary code that he reviewed "was a better source of material" than the source code that Defendants' experts relied upon. JA8892, 3159:15-17. The District Court, however, without any objection from Defendants' counsel, stopped that line of questioning, stating, "I am not going [to] let him confuse this jury with a discussion about binary code." *Id.*, 3159:21-3160:1. The District Court based this ruling on the incorrect proposition that "[n]o expert in this case has talked about binary code, including this gentleman on his direct testimony" (*id*.), when in fact, Dr. Vigna had testified about binary and assembly code during his direct and cross-examination. *See, e.g.*, JA8859-60, 3030:7-3031:4 (direct examination); JA8887, 3140:7-14; JA8889, 3147:14-19 (cross-examination). Accordingly, there was no basis to exclude Dr. Vigna's testimony as beyond the scope of his direct and cross-examinations. *See United States v. Riggi*, 951 F.2d 1368, 1375 (3d. Cir. 1991) (subject matter brought out on cross-examination is proper focus of redirect-examination).

The exclusion of Dr. Vigna's testimony regarding his review of executable code was a crucial error that allowed Defendants to unfairly discredit Finjan's validity rebuttal case. Dr. Vigna and Finjan were barred from fully responding to Defendants' incorrect argument that Dr. Vigna's analysis of the asserted prior art was superficial because it did not include a review of confidential source code. To the contrary, Dr. Vigna performed a more relevant and deeper analysis than that of Defendants' expert because he examined the actual machine executable code that provides the functionality of the prior art. JA8887, 3140:7-14; JA8889, 3147:14-19.

Defendants seized on Dr. Vigna's inability to defend the scope of his analysis and unfairly pilloried him during closing argument for his purported ignorance of how the asserted prior art actually operates. *See, e.g.,* JA8977, 3331:6-9 (Dr. Vigna "couldn't review the source code, what everybody has referred to as the 'DNA' here."); JA8979, 3339:11-21 ("[Defendants' expert] went through, and he actually presented you the source code."); JA8981, 3346:4-5 ("We showed you all the evidence. We showed you the source code."); JA8984, 3361:8-

19 ("Source code was really critical. Every other witness looked at it, except for one: Dr. Vigna"); JA8985, 3362:23-3363:5 ("he said, well, there is machine code or assembly code or something else . . . No other witness in the whole case said a word about any of that stuff. How reasonable is that?"). Defendants' attack on Dr. Vigna's credibility is vividly illustrated in the demonstrative below used during closing argument:



Credibilty of Invalidity Witnesses

Gene Spafford
Invalidity expert

Jan Hruska
Co-founder

David Klausner
Technical expert

Giovanni Vigna
Technical expert

Source code

✓ REVIEWED

Source code

NOT REVIEWED

In denying Finjan's motion for a new trial, the District Court stated that excluding this testimony was necessary to avoid jury confusion, but did not explain how this testimony would have been confusing. JA97. To the contrary, it was the exclusion of this testimony that allowed the Defendants to mislead the jury into believing that Dr. Vigna did not have a foundation to understand how the Asserted Prior Art operated.[5] Moreover, that technical testimony may be confusing to a jury is not a basis to exclude it when the underlying subject matter is inherently technical or complex. *See United States v. West*, 962 F.2d. 1243, 1248 (7th Cir. 1992) (reversing exclusion under Rule 403 of expert psychiatric testimony that was "[no] more technical or confusing" than typical testimony in other cases).

A new trial is necessary here because the Court erred in excluding Dr. Vigna's rebuttal testimony, severely prejudicing Finjan's validity rebuttal case and the credibility of its technical experts. *See Berry v. Monongahela Connecting R.R. Co.,* 397 F.2d 181, 184 (D. Del. 1967) (granting new trial based on prejudicial error as to admissibility rebuttal testimony going to truth of what witness said "in matters crucial or material to the issues on trial") (quotation and citations omitted). The District Court's error was not harmless because "it is highly probable that the

[5] In the Opinion (but not at trial), the District Court also justified the exclusion on the ground that Dr. Vigna's testimony during direct examination was not detailed regarding his review of machine code. JA98. Such detail was not needed during direct examination as Defendants had not challenged the sufficiency of his familiarity with the Accused Prior Art. Instead, Dr. Vigna explained that he reviewed the machine code to understand how the software operated and then directed the remainder of his testimony to explaining in detail his understanding of how the prior art worked based on that review. *See* JA8887, 3140:7-14; JA8889, 3147:14-19.

error [affected] the outcome of the case." *Becker v. ARCO Chem. Co.*, 207 F.3d 176, 180 (3d Cir. 2000) (granting new trial due to impactful errors in admission of evidence) (quotation omitted).

2. A New Trial is Necessary Because the Jury Verdict Was Facially Inconsistent and Ambiguous

A new trial on validity is also necessary because the jury verdict was facially inconsistent, proving that the jury was confused as to the undisputed facts, the law or both. Moreover, the jury verdict form is ambiguous as to the prior art the jury verdict was based on.

Specifically, the jury could not have logically concluded that the Asserted Claims were both (1) not infringed by Sophos and (2) invalid over Sweep-InterCheck. During the trial, Sophos' defense was based on the theory that Sweep-InterCheck, an earlier version of its accused products which Sophos alleged operated in the same way as the accused products, was prior art to and fell within the scope of the Asserted Claims. While Finjan provided extensive expert testimony distinguishing the Sophos prior art from the Asserted Claims, Sophos did not present the jury with any evidence or argument at trial that there were distinctions that would place the prior art *within* the scope and the accused products *outside* the scope of the Asserted Claims. *See* JA8871-78, 3075:17-3103:3. In contrast, Sophos did *not* dispute that its accused products were covered by Finjan's patents and its counsel admitted that "Finjan filed patents, and the

Patent Office granted patents, and ***those patent claims cover what we do***." JA8982, 3351:25-3352:2 (emphasis added). Sophos also stated that it had not "contended for a minute in this case that our products are not covered by their patents." *Id.*, 3352:3-5.

Accordingly, if the jury agreed with Sophos, it could only have found the Asserted Claims infringed but invalid. On the other hand, if the jury agreed with Finjan, it should have found the Asserted Claims valid and infringed by Sophos (based on distinctions between the accused products and the purported prior art argued by Finjan). The jury, however, could not logically find the claims invalid over Sweep-InterCheck and *not* infringed by Sophos. Yet this appears to be exactly the conclusion reached by the jury, as the jury found the Asserted Claims of the '194 Patent anticipated, and only Sweep-InterCheck was offered to show anticipation of those claims.

As the jury verdict was logically inconsistent, a new trial must be held. Under Third Circuit precedent, when a verdict is irreconcilably inconsistent on two points, as is the case here, "the appropriate remedy is ordinarily, not simply to accept one verdict and dismiss the other, but to order an entirely new trial." *Calloway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1344-45 (Fed. Cir. 2009) (vacating judgment of district court and remanding for new trial where jury verdict form reflected irreconcilable inconsistency with respect to obviousness) (applying

Third Circuit law) (quotation and citations omitted); *see also Comaper Corp. v. Antec, Inc*., 596 F.3d 1343, 1350, 1355 (Fed. Cir. 2010) (vacating judgment and remanding for new trial on invalidity due to inconsistent verdict) (applying Third Circuit law).[6]

In view of the serious deficiencies with, and logical inconsistencies in Defendants' invalidity case, a new trial is further necessitated by the fact that the jury verdict is ambiguous with respect to which prior art references invalidate each Asserted Claim and under which legal theory (anticipation, obviousness or both). Finjan submitted a proposed verdict form that requested the jurors identify any specific reference found to render a patent claim anticipated or obvious. JA8566-73; JA8902-03, 3202:10-3204:9. However, over Finjan's objections, the Court ordered the parties to file a joint verdict form that removed the question asking jurors to identify which reference was found to be anticipatory or obvious. JA8903-04, 3204:17-3208:18. Thus, it is not possible to determine what evidence the jury used to determine that the patent was invalid. *See* JA3-10.

[6] That the jury was either confused regarding invalidity or simply did not properly evaluate the issue is further confirmed by its reaching a verdict less than two hours after being instructed by the District Court that it needed to consider validity even if it had determined that the Asserted Claims were not infringed. *See* JA9388-89, 3428:23-3431:10.

3. A New Trial is Necessary Because the Jury Verdict Was Against the Clear Weight of Evidence

As set forth in more detail in Sections V(B),(C) above, JMOL or validity is warranted. Based on the evidence presented at trial, a reasonable juror could only find the Asserted Claims valid over the Asserted Prior Art because the prior art did not disclose various limitations of the Asserted Claims. In the alternative, Finjan is entitled to a new trial on validity because the jury verdict of invalidity was against the clear weight of evidence. *See, e.g., Robert Bosch, LLC v. Pylon Mfg. Corp.*, 748 F. Supp. 2d 383, 402-03 (D. Del. 2010) (rev'd on other grounds) (granting a new trial where jury's verdict of obviousness was "against the clear weight of the evidence" and based on "combinations of prior art not presented at trial"); *see also Roebuck v. Drexel Univ.*, 852 F.2d 715, 736-37 (3d Cir. 1988) (affirming grant of new trial "on the grounds that the verdict was against the great weight of the evidence.").

In contrast to this Court's review of the denial of Finjan's motion for JMOL, for purposes of a motion for a new trial, the Court need not view the evidence in the light most favorable to the verdict winner, and instead reviews the record to determine if the invalidity verdict was against the clear weight of evidence. *Norman*, 849 F. Supp. 2d at 422. Accordingly, a new trial may be warranted where the jury verdict is against the clear weight of evidence, as is the case here, even where there is sufficient evidence to preclude a grant of JMOL reversing the jury verdict. *See, e.g., Roebuck*, 852 F.2d at 736-37 (affirming grant of new trial "on the grounds that the verdict was against the great weight of the evidence," but denying request for JMOL).

A new trial on validity is also necessary to the extent this Court concludes that the District Court erred in part in denying JMOL of validity because the verdict form does not identify which set of prior art the jury relied upon in finding the Asserted Claims anticipated and obvious (e.g., NAV 95, ThunderByte, Sweep-InterCheck or some combination thereof). For example, should this Court agree that Defendants did not carry their burden to establish with clear and convincing evidence that NAV 95 anticipates the Asserted Claims of the '962 Patent, there is no way to determine if the jury's finding of invalidity of those claims was based on NAV 95, Sweep-InterCheck or both. Thus, a new trial would be necessary as the "jury has returned a general verdict and one theory of liability is not sustained by the evidence or legally sound, [therefore] the verdict cannot stand because the court cannot determine whether the jury based its verdict on an improper ground." *Wilburn v. Maritrans GP Inc.*, 139 F.3d 350, 361 (3d Cir. 1998); *see also Iacurci v. Lummus Co.*, 387 U.S. 86, 87-88 (1967) (pointing out dangers of an appellate court attempting to interpret jury verdict in light of missing findings).

V. CONCLUSION AND STATEMENT OF RELIEF SOUGHT

For the foregoing reasons, the Court should reverse the District Court's judgment of invalidity and enter judgment as a matter of law in favor of Finjan that the Asserted Claims of U.S. Patent Nos. 6,092,194 and 6,480,962 are valid. In the alternative, this Court should vacate the judgment of invalidity and remand for a new trial on the validity of the Asserted Claims of U.S. Patent Nos. 6,092,194 and 6,480,962.

Dated: December 10, 2013

Respectfully submitted,

/s/ Paul J. Andre
Paul J. Andre
Lisa Kobialka
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, California 94025
Tel: (650) 752-1700
Fax: (650) 752-1800

Attorneys For Plaintiff-Appellant
Finjan, Inc.

ADDENDUM – TABLE OF CONTENTS

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN, INC.,)
)
Plaintiff,)
)
v.)
) C.A. No. 10-cv-593 (GMS)
SYMANTEC CORP., SOPHOS, INC.,)
and WEBSENSE, INC.,)
)
Defendants.)
)

JUDGMENT

This action came before the Court for a trial by jury. The issues have been tried and the jury rendered its verdict on December 20, 2012. The verdict was accompanied by a verdict form (D.I. 746), a copy of which is attached hereto. Therefore,

IT IS HEREBY ORDERED AND ADJUDGED that judgment be and is hereby entered in favor of the defendants, SYMANTEC CORPORATION, SOPHOS, INC., and WEBSENSE, INC. (collectively, "the defendants"), and against the plaintiff, FINJAN, INC., that: SYMANTEC CORPORATION does not directly or literally infringe Claims 1, 5, 6, 12, 15, 33, 37, 38, 45, 52, or 55 of U.S. PATENT NO. 6,480,962 or Claims 1, 2, 32, 35, 36, 37, 58, 65, or 66 of U.S. PATENT NO. 6,092,194; that SOPHOS, INC. does not directly or literally infringe Claims 1, 5, 6, 12, 21, 33, 37, 38, 45, or 52 of U.S. PATENT NO. 6,480,962 or Claims 1, 2, 32, 35, 36, 37, 58, 65, or 66 of U.S. PATENT NO. 6,092,194; that WEBSENSE, INC. does not directly, literally, or willfully infringe Claims 1, 2, 32, 35, 36, 37, 58, 65, or 66 of U.S. PATENT NO. 9,092,194; that the defendants have proven by clear and convincing evidence that Claims 1, 2, 32, 35, 36, 37, 58, 65, and 66 of U.S. PATENT NO. 6,092,194 are invalid as anticipated; that the defendants have proven by clear and convincing evidence that Claims 1, 2, 32, 35, 36, 37, 58, 65, and 66 of U.S. PATENT NO. 6,092,194 are invalid as obvious; that SYMANTEC CORPORATION and/or SOPHOS have proven by clear and convincing evidence that Claims 1, 5, 6, 12, 15, 21, 33, 37, 38, 45, 52, and 55 of U.S. PATENT NO. 6,480,962 are invalid as anticipated and that Claims 1, 5, 6, 12, 15, 21, 33, 37, 38, 45, 52, and 55 are invalid as obvious.

Dec. 21, 2012

CHIEF, UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

FINJAN, INC.,

Plaintiff,

v.

SYMANTEC CORP., WEBSENSE, INC.,
and SOPHOS, INC.,

Defendants.

C.A. No. 10-cv-593 (GMS)

SPECIAL VERDICT FORM

A. Finjan, Inc.'s Infringement Claims Against Symantec Corp.

Literal Infringement of U.S. Patent No. 6,480,962

1. Do you find that Finjan has proven by a preponderance of the evidence that Symantec directly and literally infringes any of the asserted claims of U.S. Patent No. 6,480,962? *A "yes" is a finding for Finjan, a "no" is a finding for Symantec.*

YES ______ [✓ NO]

[If you answered "Yes" to Question 1], please mark the claims you found to be infringed:

Claim 1: _____ Claim 5: _____ Claim 6: _____

Claim 12: _____ Claim 15: _____ Claim 33: _____

Claim 37: _____ Claim 38: _____ Claim 45: _____

Claim 52: _____ Claim 55: _____

Literal Infringement of U.S. Patent No. 6,092,194

2. Do you find that Finjan has proven by a preponderance of the evidence that Symantec directly and literally infringes any of the asserted claims of U.S. Patent No. 6,092,194? *A "yes" is a finding for Finjan, a "no" is a finding for Symantec.*

YES ______ [✓ NO]

[If you answered "Yes" to Question 2], please mark the claims you found to be infringed:

Claim 1: _____ Claim 2: _____ Claim 32: _____

Claim 35: _____ Claim 36: _____ Claim 37: _____

Claim 58: _____ Claim 65: _____ Claim 66: _____

B. Finjan, Inc.'s Infringement Claims Against Sophos Inc.

<u>Literal Infringement of U.S. Patent No. 6,480,962</u>

3. Do you find that Finjan has proven by a preponderance of the evidence that Sophos directly and literally infringes any of the asserted claims of U.S. Patent No. 6,480,962? *A "yes" is a finding for Finjan, a "no" is a finding for Sophos.*

YES ______ NO X

[If you answered "Yes" to Question 3], please mark the claims you found to be infringed:

Claim 1: _____ Claim 5: _____ Claim 6: _____

Claim 12: _____ Claim 21: _____ Claim 33: _____

Claim 37: _____ Claim 38: _____ Claim 45: _____

Claim 52: _____

<u>Literal Infringement of U.S. Patent No. 6,092,194</u>

4. Do you find that Finjan has proven by a preponderance of the evidence that Sophos directly and literally infringes any of the asserted claims of U.S. Patent No. 6,092,194? *A "yes" is a finding for Finjan, a "no" is a finding for Sophos.*

YES ______ NO X

[If you answered "Yes" to Question 4], please mark the claims you found to be infringed:

Claim 1: _____ Claim 2: _____ Claim 32: _____

Claim 35: _____ Claim 36: _____ Claim 37: _____

Claim 58: _____ Claim 65: _____ Claim 66: _____

C. Finjan, Inc.'s Infringement Claims Against Websense, Inc.

Literal Infringement of U.S. Patent No. 6,092,194

5. Do you find that Finjan has proven by a preponderance of the evidence that Websense directly and literally infringes any of the asserted claims of U.S. Patent No. 6,092,194? *A "yes" is a finding for Finjan, a "no" is a finding for Websense.*

YES _____ NO X

[If you answered "Yes" to Question 5], please mark the claims you found to be infringed:

Claim 1: _____ Claim 2: _____ Claim 32: _____

Claim 35: _____ Claim 36: _____ Claim 37: _____

Claim 58: _____ Claim 65: _____ Claim 66: _____

Willful Infringement

6. If you answered "Yes" to Question 5, was Websense's infringement willful?

YES _____ NO X

D. Defendants' Patent Invalidity Defenses Against Finjan

Anticipation of U.S. Patent No. 6,092,194

7. Do you find that any of the Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid because they are anticipated by prior art? *A "yes" is a finding for Defendants, a "no" is a finding for Finjan.*

YES X NO

a. [If you answered "Yes" to Question 7], please identify the claims you found to be anticipated by prior art:

Claim 1: X Claim 2: X Claim 32: X
Claim 35: X Claim 36: X Claim 37: X
Claim 58: X Claim 65: X Claim 66: X

Obviousness of U.S. Patent No. 6,092,194

8. Do you find that any of the Defendants have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,092,194 are invalid because the prior art makes them obvious? *A "yes" is a finding for Defendants, a "no" is a finding for Finjan.*

YES X NO

a. [If you answered "Yes" to Question 8], please identify the claims you found to be obvious:

Claim 1: X Claim 2: X Claim 32: X
Claim 35: X Claim 36: X Claim 37: X
Claim 58: X Claim 65: X Claim 66: X

Anticipation of U.S. Patent No. 6,480,962

9. Do you find that either Symantec or Sophos have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,480,962 are invalid because they are anticipated by prior art? *A "yes" is a finding for Symantec and Sophos, a "no" is a finding for Finjan.*

YES X NO______

a. [If you answered "Yes" to Question 9], please identify the claims you found to be anticipated by prior art:

Claim 1: X Claim 5: X Claim 6: X

Claim 12: X Claim 15: X Claim 21: X

Claim 33: X Claim 37: X Claim 38: X

Claim 45: X Claim 52: X Claim 55: X

Obviousness of U.S. Patent No. 6,480,962

10. Do you find that either Symantec or Sophos have proven by clear and convincing evidence that any of the asserted claims of U.S. Patent No. 6,480,962 are invalid because the prior art makes them obvious? *A "yes" is a finding for Symantec and Sophos, a "no" is a finding for Finjan.*

YES X NO______

a. [If you answered "Yes" to Question 10], please identify the claims you found to be obvious:

Claim 1: X Claim 5: X Claim 6: X

Claim 12: X Claim 15: X Claim 21: X

Claim 33: X Claim 37: X Claim 38: X

Claim 45: X Claim 52: X Claim 55: X

E. Damages for Finjan's Patent Infringement Claims against Symantec

11. If you have found that the claims of U.S. Patent No. 6,092,194 and U.S. Patent No. 6,480,962 asserted against Symantec are either invalid or not infringed by Symantec, then you need not address damages as to Symantec. If, however, you have found at least one claim of either patent to be both valid and infringed by Symantec, what damages do you find that Finjan has proven by a preponderance of the evidence?

Lump sum royalty: $____________________

OR

Royalty rate: %____________

Royalty base: $____________

Total Damages: $____________

F. Damages for Finjan's Patent Infringement Claims against Sophos

12. If you have found that the claims of U.S. Patent No. 6,092,194 and U.S. Patent No. 6,480,962 asserted against Sophos are either invalid or not infringed by Sophos, then you need not address damages as to Sophos. If, however, you have found at least one claim of either patent to be both valid and infringed by Sophos, what damages do you find that Finjan has proven by a preponderance of the evidence?

Lump sum royalty: $____________________

OR

Royalty rate: %____________

Royalty base: $____________

Total Damages: $____________

G. Damages for Finjan's Patent Infringement Claims against Websense

13. If you have found that the claims of U.S. Patent No. 6,092,194 asserted against Websense are either invalid or not infringed by Websense, then you need not address damages as to Websense. If, however, you have found at least one claim of U.S. Patent No. 6,092,194 to be both valid and infringed by Websense, what damages do you find that Finjan has proven by a preponderance of the evidence?

Lump sum royalty: $____________________

OR

Royalty rate: %____________

Royalty base: $____________

Total Damages: $____________

REDACTED

______________________ ______________________

FOREPERSON

______________________ ______________________

______________________ ______________________

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN, INC.,

Plaintiff,

v.

SYMANTEC CORP., SOPHOS, INC.,
and WEBSENSE, INC.,

Defendants.

C.A. No. 10-cv-593 (GMS)

MEMORANDUM OPINION

I. INTRODUCTION

In this patent infringement action, plaintiff Finjan, Inc. ("Finjan" or "the plaintiff") alleges that the defendants, Symantec Corporation ("Symantec"), Sophos, Inc. ("Sophos"), and Websense, Inc. ("Websense") (collectively, "the defendants") infringe the asserted claims of the patents-in-suit.[1] (D.I. 1.) The court held a thirteen-day jury trial in this matter on December 3, 2012 through December 19, 2012. (D.I. 826-839.) At trial, each of the defendants and Finjan moved for judgment as a matter of law ("JMOL") on a number of grounds pursuant to Rule 50(a) of the Federal Rules of Civil Procedure and the court denied these motions.[2]

[1] The patents-in-suit are U.S. Patent Nos. 6,480,962 ("the '962 Patent") and 6,092,194 ("the '194 Patent"). The patents-in-suit are owned by Finjan. Finjan asserted claims 1, 5, 6, 12, 15, 33, 37, 38, 45, 52, and 55 of the '962 Patent and claims 1, 2, 32, 35, 36, 37, 58, 65, and 66 of the '194 Patent.

[2] Specifically, Sophos moved for Judgment as a Matter of Law ("JMOL") on various grounds on December 11, 2012 (D.I. 706), accompanied by an Opening Brief in Support (D.I. 707). On December 12, 2012, Symantec and Websense also filed motions for JMOL (D.I. 709; D.I. 711), accompanied by Opening Briefs in Support (D.I. 710). Finjan responded with Answering Briefs to each of these motions on December 17, 2012. (D.I. 713; D.I. 714; D.I. 15.) In addition, each of the defendants filed motions for JMOL at the close of evidence on December 18, 2012. (D.I. 724; D.I. 726; D.I. 736.) Likewise, Finjan filed JMOL motions against each of the defendants on December 19, 2012, supporting its position on various grounds. (D.I. 731; D.I. 732; D.I. 733.) Finjan also filed motions for JMOL against each of the defendants at the close of evidence on December 20, 2012. (D.I. 740; D.I. 741; D.I. 742.) The parties subsequently filed briefs in support and opposition to these motions. (D.I. 727; D.I. 737; D.I. 738; D.I. 748; D.I. 749; D.I. 750; D.I. 751; D.I. 760; D.I. 761; D.I. 765.) The court denied these motions by oral orders as they were raised throughout the trial.

On December 20, 2012, the jury returned a unanimous verdict in favor of each of the defendants on the issues of infringement with respect to each asserted claim of the patents-in-suit. (D.I. 746.) The jury further found that the asserted claims of the patents-in-suit were invalid due to obviousness and anticipation. (*Id.*) The court entered judgment on the verdict on December 21, 2012. (D.I. 747.) Presently before the court are Finjan's post-trial motions and Websense's Motion for Attorney Fees. Having considered the entire record in this case, the substantial evidence in the record, the parties' post-trial submissions, and the applicable law, the court will deny each of Finjan's post-trial motions (D.I. 770; D.I. 771; D.I. 772; D.I. 773) and Websense's attorney fees motion (D.I. 762). The court's reasoning follows.

II. BACKGROUND OF THE TECHNOLOGY

This action involves U.S. Patent Nos. 6,092,194 ("the '194 Patent") and 6,480,962 ("the '962 Patent"). Generally speaking, the patents-in-suit relate to systems and methods for protecting a computer and a network from hostile Downloadables. *See generally* '194 Patent; '962 Patent. The '194 Patent, entitled "System and Method for Protecting a Computer and Network From Hostile Downloadables," discloses a system comprised of a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. *See* '194 Patent at Abstract. The '962 Patent, entitled, "System and Method for Protecting a Client During Runtime From Hostile Downloadables," discloses a system that protects clients from hostile Downloadables and describes the system as including security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violators. The '962 Patent system includes an interface for receiving incoming Downloadables and requests made by the Downloadable, as well as a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable, and runtime events to determine whether a security police has been violated. *See* '962 Patent at Abstract. The system also includes a response engine coupled to the comparator for performing a violation-based responsive action. *Id.*

II. STANDARD OF REVIEW

Finjan asserts that it is entitled to judgment as a matter of law pursuant to Rule 50 of the Federal Rules of Civil Procedure and that a new trial is warranted under Rule 59 of the Federal Rules of Civil Procedure.

A. Renewed JMOL Motions

To prevail on a renewed motion for judgment as a matter of law following a jury trial and verdict, the moving party "must show that the jury's findings, presumed or express, are not supported by substantial evidence or, if they were, that the legal conclusion(s) implied [by] the jury's verdict cannot in law be supported by these findings." *Pannu v. Iolab Corp.*, 155 F.3d 1344, 1348 (Fed. Cir. 1998) (quoting *Perkin-Elmer Corp. v. Computervision Corp.*, 732 F.2d 888, 893 (Fed. Cir. 1984)). "Substantial evidence" is defined as "such relevant evidence from the record taken as a whole as might be accepted by a reasonable mind as adequate to support the finding under review." *Perkin-Elmer Corp.*, 732 F.2d at 893.

The court should only grant the motion "if, viewing the evidence in the light most favorable to the nonmovant and giving it the advantage of every fair and reasonable inference, there is insufficient evidence from which a jury could reasonably find liability." *Lightnin Lube, Inc. v. Witco Corp.*, 4 F.3d 1153, 1166 (3d Cir. 1993) (citing *Wittekamp v. Gulf Western Inc.*, 991 F.2d 1137, 1141 (3d Cir. 1993)). "In determining whether the evidence is sufficient to sustain liability, the court may not weigh the evidence, determine the credibility of witnesses, or substitute its version of the facts for the jury's version." *Lightning Lube*, 4 F.3d at 1166 (citing *Fineman v. Armstrong World Indus., Inc.*, 980 F.2d 171, 190 (3d Cir. 1992)). Rather, the court must resolve all conflicts of evidence in favor of the non-movant. *Williamson v. Consol. Rail Corp.*, 926 F.2d 1344, 1348 (3d Cir. 1991); *Perkin-Elmer Corp.*, 732 F.2d at 893.

"The question is not whether there is literally no evidence supporting the party against whom the motion is directed but whether there is evidence upon which the jury could properly find a verdict for that party." *Lightening Lube*, 4 F.3d at 1166 (quoting *Patzig v. O'Neil*, 577 F.2d 841, 846 (3d Cir. 1978)). Thus, a court should only grant JMOL if "the record is critically deficient of the minimum quantum of evidence." *Gomez v. Allegheny Health Servs., Inc.*, 71 F.3d 1079, 1083 (3d Cir. 1995). Importantly, in conducting the JMOL analysis, "the court may not determine the credibility of the witnesses nor 'substitute its choice for that of the jury between conflicting elements of the evidence.'" *Syngenta Seeds, Inc. v. Monsanto Co.*, 409 F. Supp. 2d 536, 539 (D. Del. 2005) (quoting *Perkin-Elmer Corp.*, 732 F.2d at 893).

B. New Trial

Pursuant to Federal Rule of Civil Procedure 59, a court may grant a new trial "for any of the reasons for which a new trial has heretofore been granted in an action at law in federal court." Fed. R. Civ. P. 59(a)(1)(A). The decision to grant or deny a new trial is within the sound discretion of the trial court. *See Allied Chem. Corp. v. Daiflon, Inc.*, 449 U.S. 33, 36 (1980). In making this determination, the trial judge should consider the overall setting of the trial, the character of the evidence, and the complexity or simplicity of the legal principles which the jury had to apply to the facts. *Lind v. Schenley Indus., Inc.*, 278 F.2d 79, 89 (3d Cir. 1960). Unlike the standard for determining judgment as a matter of law, the court need not view the evidence in the light most favorable to the verdict winner. *Allied Chem. Corp.*, 449 U.S. at 36. A court should grant a new trial in a jury case, however, only if "the verdict was against the weight of the evidence . . . [and] a miscarriage of justice would result if the verdict were to stand." *Williamson v. Conrail*, 926 F.2d 1344, 1352 (3d Cir. 1991).

C. Attorneys' Fees

In deciding whether to award attorneys' fees, the court must undertake a two-step inquiry. *See Interspiro USA, Inc. v. Figgie Intern. Inc.*, 18 F.3d 927, 933 (Fed. Cir. 1994). First, the court "must determine whether there is clear and convincing evidence that the case is 'exceptional.'" *Id.* (quotation omitted). Second, the court must determine whether "an award of attorney fees to the prevailing party is warranted." *Id.* Exceptional cases include: "inequitable conduct before the PTO; litigation misconduct; vexatious, unjustified, or otherwise bad faith litigation, frivolous suit or willful infringement." *Epcon Gas Sys., Inc. v. Bauer Compressors, Inc.*, 279 F.3d 1022, 1034 (Fed. Cir. 2002) (citation omitted).

III. DISCUSSION

A. Validity

Finjan first moves for judgment as a matter of law or, alternatively, a new trial, on validity. The court will address Finjan's motions for JMOL against each of the defendants in this section.[3] With regard to the defendants' obviousness arguments, under 35 U.S.C. § 103, a patent may not be obtained on subject matter that "would have been obvious at the time the invention was made to a person having ordinary skill in the art." 35 U.S.C. § 103. "Obviousness is a question of law based on underlying findings of fact." *In re Kubin*, 561 F.3d 1351, 1355 (Fed. Cir. 2009). Specifically, the trier of fact must consider: (1) the scope and content of the prior art; (2) the differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) secondary considerations of non-obviousness such as

[3] The court discusses Finjan's Motion for a New Trial *infra*. *See* Section III.D.

commercial success, long felt but unsolved need, failure of others, and acquiescence of others in the industry that the patent is valid, and unexpected results. *See Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966).

To determine whether an invention is patentable over the prior art, "a court must ask whether the improvement is more than the predictable use of prior elements according to their established functions." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 417, 419 (2007). In this assessment, "the invention must be considered as a whole without the benefit of hindsight, and the claims must be considered in their entirety." *Rockwell Int'l Corp. v. United States*, 147 F.3d 1358, 1364 (Fed. Cir. 1998) (citing *W.L. Gore & Assocs. v. Garlock, Inc.*, 721 F.2d 1540, 1551 (Fed. Cir. 1983); *Medtronic, Inc. v. Cardiac Pacemakers, Inc.*, 721 F.2d 1563, 1567 (Fed. Cir. 1983)). Invalidity by "anticipation requires that the four corners of a single[] prior art document describe every element of the claimed invention, either expressly or impliedly, such that a person of ordinary skill in the art could practice the invention without undue experimentation." *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1271, 1282 (Fed. Cir. 2000).

When challenging the validity of a patent for obviousness based on a combination of prior art references, the challenger bears the burden of proving, by clear and convincing evidence, that one of ordinary skill in the art would have had reason to attempt to make the combination and would have had a reasonable expectation of success in doing so. *PharmaStem Therapeutics, Inc. v. ViaCell, Inc.*, 491 F.3d 1342, 1360 (Fed. Cir. 2007). A defendant must prove invalidity by clear and convincing evidence and the ultimate burden of persuasion never shifts to the plaintiff. *See Pfizer, Inc. v. Teva Pharm. U.S.A., Inc.*, 882 F. Supp. 2d 643, 700 (D. Del. 2012).

1. Obviousness

As noted, Finjan has filed motions for JMOL against each defendant and has submitted separate briefs in support. Because there is overlap in the obviousness arguments advanced at trial and discussed in these briefs by each defendant and Finjan, the court combines its discussion here. Where a prior art reference was argued by only one defendant, the court makes note of this distinction.

At trial, the defendants presented prior art references and, in light of these references, the jury concluded that the '194 and '962 Patents are invalid. In its motions for JMOL as to obviousness, Finjan asserts that the jury verdict should be set aside because: (1) the ThunderByte reference is not prior art to the '194 Patent and, even if it were, the asserted claims of the '194 Patent are valid over ThunderByte and all other references Symantec presented; and (2) Norton Antivirus 95 ("NAV 95") is not prior art to the '962 Patent and, even if it were, the asserted claims of the '962 Patent are valid over NAV 95 and all other references Symantec presented. (D.I. 791 at 1 (citing D.I. 732 at 2-5, 6-10; D.I. 742 at 2-4, 4-7).) The court addresses each argument separately below.

a. *The '194 Patent: Prior Art References ThunderByte 7.0 & MIMESweeper*

At trial, Symantec argued that the '194 Patent is invalid as obvious in light of prior art references ThunderByte 7.0 and MIMESweeper. Specifically, Symantec asserted that MIMESweeper is a gateway product that was designed for use with ThunderByte and, when combined as described in the MIMESweeper literature, the prior art technology would scan email attachments at the gateway. (D.I. 808 at 5 (citing Tr. at 2141:22-2143:8, 2147:2-2148:23).) During the scanning process, according to the defendants, ThunderByte would extract a list of suspicious computer operations from a Downloadable and compare that list to a security policy. (*Id.* (citing Tr. at 2149:6-2152:15).) If the security policy was violated, ThunderByte could then delete the Downloadable, preventing execution at the client. (*Id.* at 5-6 (citing Tr. at 2152:16-2153:6).) Symantec asserts that the jury verdict of invalidity based on ThunderByte and MIMESweeper should not be overturned because: (1) there was substantial evidence that ThunderByte 7.0 qualifies as prior art; (2) the defendants were not required to demonstrate that ThunrderByte and MIMESweeper were enabled; (3) a person of ordinary skill in the art could have combined ThunderByte and MIMESweeper; and (4) the ThunderByte/MIMESweeper combination disclosed the disputed elements of the asserted claims of the '194 Patent.

Conversely, Finjan asserts that the ThunderByte reference is not prior art to the '194 Patent and, even if it were, the asserted claims of the '194 Patent are valid over ThunderByte and all other references presented by Symantec and Websense. (D.I. 791 at 1 (citing D.I. 732 at 2-5; *see also* D.I. 742 at 2-4).) Specifically, Finjan asserts that Symantec and Websense's obviousness argument are fundamentally flawed, necessitating JMOL, because the defendants failed to prove that: (1) ThunderByte 7.0 was available in the United States before the '194 Patent's November 8, 1996 priority date; (2) the source code and manuals they relied upon were specifically for ThunderByte 7.0; (3) the ThunderByte and MIMESweeper manuals relied upon were enabled; (4) a person of ordinary skill in the art could have combined ThunderByte and MIMESweeper, let alone would have been motivated to do so; and (5) ThunderByte 7.0 and MIMESweeper disclosed the limitations of the asserted claims. (*Id.* at 3.)

i. *ThunderBYTE 7.0's Availability in the United States*

Finjan argues that Symantec has failed to satisfy its burden of proving by clear and convincing evidence that ThunderBYTE 7.0 was available in the United States before November 8, 1996. (D.I. 791 at 3) Specifically, Finjan asserts that the testimony of Dr. Spafford, Symantec's validity expert, was insufficient to demonstrate the prior art's availability and that, because Symantec's only witness who could establish availability was precluded from testifying as a sanction for improper assertions of privilege during his depositions, Symantec could not make this showing.[4] (*Id.* at 3-4 (citing Tr. at 2054:5-8).) With regard to Dr. Spafford, Finjan notes that he testified that a British Virus Bulletin contained a review of ThunderByte. Finjan maintains that this testimony is insufficient because the British article failed to: disclose when, if ever, ThunderByte, the product of a Netherlands company, was commercially available in the United States; demonstrate that the review was of a commercial version of ThunderByte; prove that ThunderByte, if available at all, was available outside of the Netherlands or Britain; and demonstrate that the version reviewed can prove availability, particularly where the article noted that the review was limited to a "demonstration version" and that there was "no serial number visible." (*Id.* at 4 (citing DX 4708-21; DX 4708-23).)

Finjan further notes that it objected to Dr. Spafford's testimony on ThunderByte as lacking foundation, but that the court permitted him to testify so long as Symantec's counsel would not ask him to opine on the availability of ThunderByte in the United States. (*Id.* (citing Tr. at 2137:13-2140:10).) While Symantec's counsel did not question Dr. Spafford on this issue, he did testify during his direct examination and without provocation, that "[t]he ThunderByte program is an antivirus program that was available in early 1996." (*Id.* at 4-5 (citing Tr. at 2140:19-20).) Finjan details that the court denied its objection without prejudice and that it raises the objection again here because that testimony was: (1) outside the scope of the agreement reached between the court and counsel; (2) entirely lacking in foundation due to the

[4] Finjan states that Symantec's counsel acknowledged to the court on the record that it could not prove the availability of ThunderByte 7.0 as prior art without Dr. Slade's testimony. Specifically, Finjan notes that Symantec's counsel stated, in response to the court's question as to whether Symantec has "another way to prove what you are attempting to prove," "No, Your Honor." (D.I. 791 at 4 (citing Tr. at 2051:10-14).)

preclusion of Mr. Slade's testimony and Dr. Spafford's own lack of personal knowledge; and (3) outside the scope of Dr. Spafford's expert report.[5] (*Id.* at 5 (citing Tr. 2139:5-2140:7); *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 973-74 (E.D. Mich. 2003)).) Moreover, Finjan contends that Symantec cannot rely on the copyright notice in the ThunderByte manual to establish availability in the United States, because: it is inadmissible hearsay; shows only that ThunderByte was available in the Netherlands; and this notice fails as a matter of law to demonstrate clearly and convincingly that the product was known or used by others prior to the critical date. (*Id.* (citing *Hilgraeve*, 271 F. Supp. 2d at 975; DJX-371-2).)

Finjan further argues that the "date modified" information contained in the source code and on which Dr. Spafford relied is irrelevant because this evidence demonstrates only that the source code "was being edited on that date, but does not establish when, if ever, it became available in the United States." (*Id.* at 6.) In fact, Finjan notes that other files on the ThunderByte CD "had purported modified dates as late as October 16, 1996" and, even assuming that ThunderByte files were still being modified on that date, "it is highly unlikely they were then made available in the United States less than a month later." (*Id.*) Finally, Finjan contends that Symantec has failed to provide foundational evidence linking the source code and manuals on which it relied to the version of ThunderByte asserted here—ThunderByte 7.0. Specifically, Finjan asserts that the manual about which Dr. Spafford testified did not identify the version of

[5] With regard to Finjan's request to strike Dr. Spafford's statement, the court agrees with Symantec that Finjan has suffered no prejudice. Specifically, following a sidebar in which the court decided that Symantec could not elicit testimony from Dr. Spafford regarding whether he understood ThunderByte to be publicly available in the United States, Dr. Spafford testified, without provocation, that ThunderBYTE 7.0 was, in fact, publicly available. *See* Tr. at 2140:15-23. Dr. Spafford was not privy to the court's instruction to counsel at sidebar. Moreover, Symantec counsel indicated at sidebar that, should Dr. Spafford make such a statement as to ThunderByte 7.0's availability, he would interrupt the testimony. Indeed, immediately after Dr. Spafford's comment on availability, Symantec's counsel instructed him that "[w]e don't need to talk about availability issues." *See id.* at 2140:16-24. Further, Symantec did not rely on Dr. Spafford's statement during closing arguments as proof that ThunderByte 7.0 was available. Instead, and as Symantec's counsel indicated he would do at sidebar, the questioning of Dr. Spafford was limited to eliciting certain facts, such as the Virus Bulletin, the copyright dates, and the dates modified of the software he examined. *See id.* at 2140:15-2141:2, 2144:9-2146:13, 2205:3-6. In view of the foregoing, the court declines to grant Finjan's request and does not strike the testimony in question.

ThunderByte it corresponds to and, without this evidence, cannot establish relevancy. (*Id.* at 6-7.)

In light of the evidence presented at trial, however, the court concludes that Symantec introduced substantial evidence sufficient to support a jury verdict of invalidity as to the '194 Patent. The court reviews each piece of evidence below. Dr. Spafford, Symantec's invalidity expert, testified at length about his review and analysis of the ThunderByte 7.0 software product, which was produced in native form as exhibit DJX-368.[6] (*Id.* at 2 (citing Tr. at 2140:16-2141:5, 2144:9-24; DJX-368).) The directory containing this software product was titled "TBAV 7.00" and, as Dr. Spafford testified, the date modified for the files he used was February 8, 1996. (*Id.* at 3 (citing Tr. at 2144:9-24, 2089:9-12; SYMDX9-54).) Dr. Spafford also relied on a user manual contained in DJX-368, which bears a copyright date of 1996. (*Id.* (citing DJX-371-2; Tr. at 2146:20-22).)

In addition, Symantec asserts and the court agrees that, in consideration of the following evidence, the jury could have reasonably found that ThunderByte 7.0 is prior art under 35 U.S.C. § 102(a)-(b) because it was known, used, sold, and on sale in the United States before November 8, 1996. First, Symantec introduced a press release from February 9, 1996 (DX-4348), which was released by ThunderBYTE and CompuServe and announced that ThunderBYTE 7.0 "will be

[6] Dr. Spafford described DJX-368 in his direct examination testimony:

> Q: When you loaded those files, did the files have any information concerning when they were last modified?
> A: The information that I had in the directory is as shown in this top window, and showed February 8, 1996.
> Q: So DJX-368, can you tell us what that is?
> A: That's a listing of the contents on the CD, the files that were on it—not the complete list, but the first few showing the date.
> Q: Now, if we looked at DJX-368 in its entirety, would we see the dates for the rest of the files?
> A: Yes.
> Q: And do you recall what those dates were?
> A: They were the same.

Id. at 2144:9-24.

released on CompuServe immediately," and that "users around-the-world can download a free, 30-day, fully-functional trial version of TBAV from CompuServe on the Windows 95 Support Menu." (*Id.* (citing DX-4348-1).) The press release also quotes an employee from CompuServe located in Columbus, Ohio, who discusses the benefits of ThunderByte 7.0, and the Director of Technical Support for ThunderByte in North America. (*Id.* (citing DX-4348-1-2).) Moreover, the date of the press release corresponds to the day after the date modified of the ThunderByte 7.0 software that Dr. Spafford tested and relied upon in assessing invalidity. The press release was loaded into the Lexis-Nexis database on February 10, 1996. (*Id.* (citing Tr. at 2144:9-24; DX-4348-3).)

Finjan states that it objected to the introduction of this evidence when Symantec presented it to Dr. Vigna during Finjan's rebuttal validity case. (D.I. 791 at 4 n.4.) Finjan did object when Symantec asked Dr. Vigna about the document as being "[o]utside the scope" of the direct examination and the court overruled the objection. Tr. at 3132:9-13. Finjan renews the objection at this stage, and argues that the evidence should not be considered for JMOL purposes because it was introduced after the close of Symantec's case. The court disagrees. "In entertaining a motion for judgment as a matter of law, the court should review all of the evidence in the record[,]" which would include DX-4348. *See Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000). The court also rejects Finjan's contention that Symantec did not authenticate this document because, as noted, the press release was included in the Lexis-Nexis database. *See* Fed. R. Evid. 902(6) (stating that documents such as press releases from sources whose accuracy cannot reasonably be questioned are self-authenticating); *see also In re UnumProvident Corp. Sec. Litig.*, 396 F. Supp. 2d 858, 876-77 (E.D. Tenn. 2005). Symantec also asserts and the court agrees that Finjan waived this argument because it did not object to

DX-4348 on hearsay or authentication grounds. (D.I. 810 at 4 (citing Tr. at 3132:9-14).) Moreover, while Finjan asserts that the press release does not prove availability, the release notes that ThunderByte 7.0 "will be released on CompuServe immediately." (*Id.* (citing DX-4348-1).)

Second, Symantec also presented a 1996 user manual for ThunderByte 7.0 (DJX-371), which notes that the product's developer (ESaSS) maintained "ThunderBYTE support Bulletin Board Systems" containing "updates" and "complete releases" for the product. (*Id.* (citing DJX-371-26, -27, -89).) Though Finjan asserts that this manual shows only that ThunderByte was available in the Netherlands, Symantec argued that the manual contradicts this assertion because it describes: (1) online "ThunderB[yte] support Bulletin Board Systems" that contained "updates" and "complete releases" for the product; and (2) a ThunderByte "U.S. support site." (*Id.* at 5 (citing DJX-371-26, -27, -89).) Thus, Symantec maintains, because of availability online, this version of ThunderByte 7.0 was accessible to people in the United States who had modems and could access online bulletin board systems, including users of online services such as CompuServe. In addition, the 1996 user manual expressly states that in order "to maintain the highest reliability' of these bulletin boards, "the Dutch and U.S. ThunderB[yte] support sites issue regular beta releases, also containing only the files that have changed." (*Id.* at 3 (citing DJX-371-27).)

In response to Finjan's contention that the 1996 copyright date in the user manual is inadmissible hearsay, Symantec argues that here, unlike in the *Hilgraeve* case on which Finjan relies, it introduced additional evidence regarding the availability of ThunderByte 7.0, including the February 1996 press release, the May 1996 Virus Bulletin, discussed below, and the availability of prior versions to persons within the United States. In addition, Dr. Spafford expressly linked the user manual to the ThunderByte 7.0 software on which he relied. (*Id.* at 5 (citing Tr. at 2140:25-2141:5, 2146:20-22)); *see also Rackable Sys., Inc. v. Super Micro Computer, Inc.*, 2007 WL 1223807, at *23 (N.D. Cal. 2007) (distinguishing the *Hilgraeve* case to cases where other evidence exists besides the copyright date for demonstrating public availability).

Third, Symantec introduced a May 1996 Virus Bulletin (DX-4708), which contains a review for ThunderByte 7.0, the same version Dr. Spafford used in conducting his analysis. (*Id.* (citing Tr. at 2144:25-2146:22; DX-4708-23).) In fact, Dr. Spafford testified that he was on the editorial board for the Virus Bulletin at that time and received complimentary copies of the publication. (*Id.* (citing Tr. at 2411:25-2145:25).) In response to Finjan's assertion that the Bulletin did not demonstrate that ThunderByte 7.0 was available in the United States or even commercially available, Symantec notes that the jury was presented with evidence that the Bulletin review provided pricing information for the product and that it was sent to individuals in the United States. (*Id.* at 6 (citing DX-4708-24).)

Fourth, Symantec engineer, Cary Nachenberg, also testified that he tested ThunderByte version 6.34 in connection with his master's thesis at UCLA. (*Id.* (citing Tr. at 1832:16-1833:2; DX-4011).) Mr. Nachenberg testified that "ThunderByte was a competing antivirus product with Symantec's products." (*Id.* (citing Tr. at 1832:5-1832:8).) Mr. Nachenberg also explained that, during the prosecution of a patent that he obtained for work related to his thesis, the 1995 user manual for ThunderByte was cited to the PTO, and the tests he performed on version 6.34 of ThunderByte are described in the patent specification. (*Id.* (citing Tr. at 1831:7-1833:2; DX-4713-2, -12:31-50).)

Fifth, Dr. Spafford discussed a July 18, 1995 article from the Computer Business Review (DJX-122), which states that the MIMESweeper product "comes with interfaces for virus protection packages such as Dr. Solomon's, ThunderB[yte] and F-Prot[.]" (*Id.* at 4 (citing DJX-122; Tr. at 2141:24-2142:4, 2143:9-17).) He also testified about a June 30, 1995 article, which discussed the release of MIMESweeper and the "built in interfaces" on that email gateway product "for virus packages, including ThunderB[yte]." (*Id.* (citing DJX-125; Tr. at 2141:24-2143:8).) Sixth, Symantec introduced a September 1995 article by David Stang, who worked at Norman Data Defense Systems in Fairfax, Virginia, which states that "[p]roducts of note which offer heuristic scanning include TBScan (from ESaSS)" and also includes an appendix showing the results of an experiment that Mr. Stang performed using version 6.24 of ThunderByte. (*Id.* (citing PTX-0005-1, -9, -12).) Symantec argues that Mr. Nachenberg's testimony and the MIMESweeper and Stang articles support the jury verdict. (*Id.* at 6 (citing *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1569 (Fed. Cir. 1988) ("Evidence of routine business practice can be sufficient to prove that a reference was made accessible before a critical date.")).)

Finally, and in response to Finjan's assertion that the CD Mr. Slade provided had files with dates modified after February 8, 1996, Symantec notes that all of the files upon which Dr. Spafford relied had in the "TBAV 7.00" folder had the February 1996 date as the date modified. (*Id.* at 6 (citing Tr. at 2144:9-24; DJX-368).) Moreover, Symantec counters Finjan's argument that it conceded that it had no other evidence regarding the public availability of ThunderByte 7.0 outside Mr. Slade's testimony. Specifically, Symantec notes that, while Finjan is correct it had no other evidence as to how the CD Mr. Slade provided was prepared or his role as a product reviewer at the relevant time, it presented other evidence regarding public availability, including the multiple references detailed above and the Virus Bulletin, which Symantec notes that it identified at sidebar. (*Id.* (citing Tr. at 2138:11-2139:23).)

ii. *Enablement: ThunderByte and MIMESweeper*

Finjan contends that Symantec's invalidity case also fails because Dr. Spafford "did not offer any evidence that the purported teachings of the [ThunderByteand MIMESweeper] manuals were enabled." (*Id.* (citing D.I. 791 at 7).) However, as Syamtec correctly notes, Dr. Spafford relied on these manuals as evidence of how the products themselves functioned and that it was the products that were the basis of his obviousness opinions. *See, e.g.*, Tr. at 2154:8-13, 2161:8-2162:3. Indeed, Dr. Spafford was not required to demonstrate that the user manuals were enabling as part of his obviousness analysis. *See Geo. M. Marin Co. v. Alliance Machine Sys. Int'l LLC*, 618 F.3d 1294, 1302 (Fed. Cir. 2010) ("Under an obviousness analysis, a reference need not work to qualify as prior art; 'it qualifies as prior art, regardless, for whatever is disclosed therein.'" (citation omitted)); *Zenith Elecs. Corp. v. PDI Commc'n Sys., Inc.*, 522 F.3d 1348, 1356 (Fed. Cir. 2008) ("[T]he public use itself need not be enabling."). Finjan's assertion is also inconsistent with its pretrial representation that it "will not offer Dr. Vigna's limited testimony regarding the non-enablement of third-party software products." (D.I. 672 at 1.) Thus, Dr. Spafford's reliance on executable software and user manuals for the publicly-available products as part of his obviousness analysis was appropriate.

iii. *Whether a Person of Ordinary Skill in the Art Could Have Combined ThunderByte and MIMESweeper*

Finjan also challenges the jury verdict in asserting that a person of ordinary skill in the art could not have combined ThunderByte 7.0 and MIMESweeper as Symantec proposes and, further, that a skilled artisan would not have been motivated to do so. (D.I. 791 at 7.) Specifically, Finjan notes that Symantec relied on an article stating that MIMESweeper, which is based on a Windows NT platform, has a "built-in interface" for ThunderByte, as proof that such a combination would have been technically possible and obvious. (*Id.* (citing Ex. 34; DJX-125; Tr. at 2142:21-2143:17).) Finjan notes that Dr. Vigna conducted experiments showing that

ThunderByte 7.0 was not compatible with the Windows NT System and that Symantec did not cross-examine Dr. Vigna on this testimony or challenge his conclusion. (*Id.* at 7-8 (citing Tr. at 3059:23-3062:8, 3069:1-11).) Further, Finjan notes that Symantec relied on two non-technical articles stating that MIMESweeper could be combined with ThunderByte by using ThunderByte to scan email attachments. (*Id.* at 8.) Finjan maintains that these articles do not demonstrate Symantec's claim because, to yield the inventions, "it would be necessary to combine ThunderByte's heuristic scanning with MIMESweeper (i.e., using MIMESweeper as a gateway), which is not discussed in the articles." (*Id.* (citing Tr. at 3061:15-3065:21-3066:5).) According to Finjan, these articles only suggest a plan to make MIMESweeper compatible with certain versions of ThunderByte and Symantec did not prove clearly and convincingly that MIMESweeper could be combined with the 7.0 version of ThunderByte. (*Id.*)

However, Symantec did, in fact, present expert testimony that the products could be combined. Specifically, Dr. Spafford testified as to this conclusion by relying on press releases noting that MIMESweeper "comes with interfaces for virus protection package such as . . . ThunderByte" and identified excerpts from the MIMESweeper user manual that discuss virus scanning at the email gateway. (D.I. 810 at 7 (citing Tr. at 2141:24-2143:17, 2146:23-2147:24; DJX-122; DJX-125-5, -75).) In addition, Symantec questioned Dr. Vigna on cross-examination as to whether he used the MIMESweeper product in his experiment and he indicated that he did not because it was not available. (*Id.* (citing Tr. at 3131:5-10).) Notably, while Finjan argues that Symantec failed to provide the jury with substantial evidence to counter Dr. Vigna's conclusion or to show that Dr. Spafford had personal knowledge regarding whether it was possible to combine the two products, neither expert conducted an experiment with both products. The jury was free to consider the testimony of each expert, weigh the credibility of their opinions, and conclude that Symantec demonstrated this element.

iv. *Whether the ThunderByte/MIMESweeper Combination Discloses the Disputed Elements of the Asserted Claims*

Finjan's final argument is that the ThunderByte/MIMESweeper combination does not disclose the asserted claims of the '194 Patent. Specifically, Finjan asserts that Symantec failed to prove that ThunderByte discloses use of "security profile data," including a "list of suspicious computer operations" used to identify potentially harmful Downloadables because ThunderByte "only looked at file characteristics, not operations." (D.I. 791 at 8 (citing Tr. at 3062:9-3067:8).) As a result, Finjan maintains that ThunderByte only analyzed attributes of a file, not what the file was doing, such that it did not use the claimed "security profile data" and could not satisfy related limitations of comparing file operations against security policies and preventing execution of the Downloadable if a security policy is violated. Regarding the "preventing execution of the Downloadable by the client if the security policy has been violated" claim limitation, Finjan contends that ThunderByte automatically deleted or prompted the user to delete a suspicious file without performing an analysis of the file's operations. (*Id.* at 9 (citing Tr. at 2152:16-2153:13).) Thus, ThunderByte, Finjan argues, was not capable of blocking a suspicious file from executing based on a comparison to a security policy. (*Id.*)

Moreover, Finjan maintains that ThunderByte, alone or in combination with MIMESweeper, was not capable of detecting suspicious operations in JavaScript or Visual Basic script within the Downloadable, as required by asserted Claims 35 and 36 of the '194 Patent. (*Id.* (citing Tr. at 3069:12-21).) In particular, Finjan cites to Dr. Spafford's testimony that, although ThunderByte did not mention JavaScript or Visual Basic script, a person of ordinary skill in the art would have considered it obvious to modify ThunderByte to process such files.

(*Id.* (citing Tr. at 2193:2-11, 2160:5-2161:19).) Finjan notes that Dr. Spafford did not identify a prior art reference with which ThunderByte and MIMESweeper could be combined to yield this result or the motivation behind the combination of such a reference with ThunderByte/MIMESweeper. (*Id.*) Therefore, Finjan contends that Symantec failed to establish a *prima facie* case of invalidity, as conclusory *ipse dixit* analysis "cannot be enough to constitute clear and convincing evidence in an obviousness case." (*Id.* (citing *Cephalon, Inc. v. Watson Pharms, Inc.*, No. 2011-1325, 2013 WL 538507, at *6 (Fed. Cir. Feb. 14, 2013) (concluding that *ipse dixit* statements by an expert are insufficient to sustain an invalidity case)); D.I. 819 at 5 (citing *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1366-67 (Fed. Cir. 2012) (stating that differences between asserted prior art and claimed elements supported the reversal of a finding of obviousness)).)

The court disagrees with Finjan's contention that Symantec failed to present substantial evidence on which the jury could rely to conclude that the ThunderByte/MIMESweeper combination disclosed the disputed elements of the asserted claims. Specifically, and with regard to the "list of suspicious operations" element, Dr. Spafford testified in detail how ThunderByte 7.0 identified a list of suspicious computer operations. *See* Tr. at 2148:24-2151:9, 2151:15-2152:15, 2153:14-2154:7. Dr. Spafford also cited to excerpts from the user manual that the program will disassemble files to detect suspicious instruction sequences. *See id.* at 2148:24-2151:9; DJX-371-8 ("TbScan will disassemble files. This makes it possible to detect suspicious instruction sequences and detect yet unknown viruses."); DJX-371-161 ("By looking into the file's contents and interpreting the instructions, TbScan is able to detect the purpose of these instructions."). Moreover, Dr. Spafford also described the results of experiments that he conducted in forming his conclusion and discussed a screen shot showing some of the identified suspicious operations. (D.I. 810 at 8 (citing Tr. at 2153:14-2154:7; SYMDX9-61).)

Regarding the "preventing execution of the Downloadable" limitation, Symantec also presented substantial evidence that this element was met by the ThunderByte/MIMESweeper combination, including Dr. Spafford's testimony and experiments and the ThunderByte user manual. (*Id.* (citing Tr. at 2152:16-2154:13; DJX-371-64, -65; SYMDX9-61).) In addition, and contrary to Finjan's assertions, Dr. Spafford also demonstrated that, in determining whether to prevent execution, ThunderByte 7.0 analyzed the operations of the policy and then compared them to a policy. *See* Tr. at 2148:24-2152:15; DJX-371-161. Thus, the jury was presented with Dr. Spafford's opinion that ThunderByte did, in fact, meet the asserted claim.

Finally, the court finds that Symantec presented substantial evidence that it would have been obvious to use the ThunderByte/MIMESweeper combination to detect malicious operations in JavaScript and Visual Basic script. *See* Tr. at 2159:4-2162:3; DJX-371-63. While Finjan is correct that ThunderByte did not mention JavaScript or Visual Basic script, the evidence Symantec presented that it would have been obvious to use JavaScript or Visual Basic script constituted more than a "conclusory *ipse dixit*" analysis. Specifically, Dr. Spafford testified that these scripts were developed by others and were known before the claimed invention. *See* Tr. at 429:8-430:4, 2160:24-2161:7, 2499:1-5; PTX-0001. Indeed, Dr. Spafford testified that the ThunderByte product contemplated scanning files in different languages. (D.I. 810 at 9 (citing DJX-371-63).) Dr. Spafford testified that, according to the principle of defense in depth, it would have been obvious to use ThunderByte to scan for viruses in these scripts, which he explained may be attached to emails. (*Id.* (citing Tr. at 2159:4-2162:3, 2091:4-2092:20).) Dr.

Spafford also stated that he expressed concern about viruses attached to these scripts to the developers of the MIME standard used in MIMESweeper. (*Id.* (citing Tr. at 2160:24-2161:7).)

In consideration of the evidence detailed above, the court concludes that Symantec presented substantial evidence that, if found credible, could reasonably support an invalidity verdict.

b. *The '962 Patent: Prior Art References NAV 95 & HotJava*

Finjan next argues that the court should grant JMOL overturning the jury's verdict that the '962 Patent is invalid over NAV 95 and other references Symantec presented. Finjan notes that Symantec argued that the asserted claims of the '962 Patent were anticipated by NAV 95, with the exception of Claim 52, which is alleged to be obvious in view of NAV 95 combined with HotJava. Finjan asserts that Symantec improperly relied on a combination of items to allege anticipation based on NAV 95 and failed to show that: (1) NAV 95 and HotJava were available in the United States prior to November 8, 1996; (2) the NAV 95 manuals relied upon were enabled[7]; and (3) NAV 95 disclosed the limitations of the asserted claims. (D.I. 791 at 10.) Specifically, Finjan states that Symantec "improperly relied on a combination of purportedly related materials including Norton Antivirus software, source code, and a user manual," and that Dr. Spafford "relied on a mix of the NAV 95 Software, Source Code, and Manual that varied from limitation to limitation." (*Id.*) Finjan contends that, because each "are admittedly distinct items of prior art, [Dr.] Spafford's opinion that they anticipate the asserted claims in combination fails as a matter of law." (*Id.* at 10-11.) Thus, because, according to Finjan, Dr. Spafford offered no obviousness analysis for the asserted claims of the '962 Patent, except for Claim 52 with

[7] For the reasons stated above in Section III.A.1.a.iii, the court disagrees with Finjan's assertion that Symantec had to demonstrate that the prior art was enabled. Specifically, Finjan agreed prior to trial not to raise any issue concerning the enablement of prior art software products. *See supra* Section III.A.1.a.iii. In addition, because Dr. Spafford relied upon the NAV 95 product, Finjan's argument that he failed to show enablement of the NAV 95 user manual is irrelevant. *See id.*

respect to HotJava, no reasonable jury could find that the asserted claims are invalid in view of NAV 95. (*Id.* at 11.)

First, Finjan argues that Symantec failed to make the threshold showing that NAV 95 and HotJava were publicly available in the United States prior to November 8, 1996. Specifically, Finjan asserts that Symantec improperly sought to demonstrate public availability of NAV 95 in the United States by offering the uncorroborated testimony of two company employees, Symantec Vice President, Carey Nachenberg, and Symantec engineer, Mark Kennedy, and offered no documents in support. (*Id.* (citing *Lacks Indus., Inc. v. McKechnie Vehicle Componenets USA, Inc.*, 322 F.3d 1335, 1349-50 (Fed. Cir. 2003) (concluding that "oral testimony by interested parties must be corroborated by documentary testimony" and noting that the testimony of one interested witness cannot be used to corroborate the testimony of another witness)).) With respect to HotJava, Finjan maintains that Symantec relied exclusively on the testimony of Jeffrey Nisewanger, who stated that HotJava was not commercially released until March 1997 and that, prior to this date, HotJava was only available in pre-beta form—a release "that is for internal consumption and not something that you would sell as a product to the public." (*Id.* at 12 (citing Tr. at 2063:11-23, 2128:17-21, 2186:19-25, 3054:11-17).)

Second, Finjan asserts that Symantec did not demonstrate by clear and convincing evidence that NAV 95 discloses the limitations of the asserted claims of the '962 Patent. In particular, Finjan argues that NAV 95 cannot invalidate because it did not monitor a "plurality of subsystems" of an operating system and, instead, only monitored filed systems. (*Id.* at 13.) Finjan notes that Dr. Vigna provided unrebutted testimony that the "input/output" monitoring of NAV 95 was limited to "disk space orientation [e.g., to] format the hard drive, modify the file, modify an attribute of an executable file," all of which are operations of a file system. (*Id.*

(citing Tr. at 3036:14-3037:7, 3025:4-12, 3040:15-3043:4).) Next, Finjan claims that NAV 95 did not practice the step of "performing a predetermined responsive action based on the comparison." In support, Finjan cites to the testimony of Dr. Spafford and Websense's non-infringement expert, Ms. Frederiksen-Cross, to demonstrate that "the measures that NAV 95 took based on the rules (e.g., blocking an action or prompting the user) were performed exclusively based on the action being performed (e.g., reformatting the hard drive), and were not in response to the comparison of any information about Downloadables to any policies."[8] (*Id.* at 14-15 (citing Tr. at 3045:14-3046:5).) Thus, Finjan argues that NAV 95 did not perform this limitation because the identity of the Downloadable performing the action was unknown. (*Id.*)

Finally, Finjan contends that a person of ordinary skill in the art would not have been motivated to combine NAV 95 and HotJava in the "hodge-lodge fashion" Dr. Spafford proposed and, therefore, that Symantec failed to prove invalidity of Claim 52. Specifically, Finjan maintains that there would have been no motivation to combine the two programs because they were directed to different tasks—HotJava monitored Java applets run by a web browser and NAV 95 monitored file systems. (*Id.* at 15 (citing Tr. at 3051:22-3053:2).) Moreover, Finjan argues that Claim 52 is not invalid because these products did not monitor "an operating system" and NAV 95 did not perform the "adding information pertaining to the Downloadable to a suspicious Downloadable database" as required by Claim 55. (*Id.* (citing Tr. at 3048:8-15, 3050:23-3051:21).) Thus, Finjan asserts that Symantec failed to present substantial evidence from which a reasonable jury could find that it proved invalidity clearly and convincingly.

[8] Finjan argues that Drs. Spafford and Ms. Frederiksen-Cross' testimony demonstrated that NAV 95 simply blocked certain actions, regardless of the sources performing the action, and did not, therefore, perform the comparison to a security policy of information that "pertain[s] to the Downloadable." (D.I. 791 at 14 (citing Tr. at 2110:7-2111:11, 2867:13-19, 3027:21-3029:4, 3037:16-24, 3043:5-3045:13).)

In view of the record before it, the court disagrees. First, regarding Finjan's assertion that Symantec improperly premised its anticipation argument on a combination of references, under relevant law it was appropriate for Dr. Spafford to rely on the NAV 95 executable software, user manual, and source code to show how NAV 95 operated. Specifically, and as Symantec correctly notes, where, as here, a product is alleged to anticipate, the fact that "the offered product is in fact the claimed invention may be established by any relevant evidence, such as memoranda, drawings, correspondence, and testimony of witnesses." (D.I. 810 at 9-10 (citing *Laboratory Skin Care, Inc. v. Limited Brands, Inc.*, 2011 WL 4005444, at *5 (D. Del. Sept. 8, 2011) (citing *Sonoscan, Inc. v. Sonotek, Inc.*, 936 F.2d 1261, 1263 (Fed. Cir. 1991)).) In fact, the NAV 95 software product upon which Dr. Spafford relied included both the executable software and a copy of the user guide explaining how the product worked. (*Id.* at 10 (citing Tr. at 2098:4-9; *Zenith Elecs.*, 522 F.3d at 1358; *Unitherm Food Sys., Inc. v. Swift-Eckrich, Inc.*, 375 F.3d 1341, 1352 (Fed. Cir. 2004)).)

In addition, Finjan's claims that Dr. Spafford testified that the NAV 95 manual was considered by the Patent Office and that the user guide is a different piece of prior art than the source code and software, is not supported by the record. (D.I. 791 at 11.) With regard to Dr. Spafford's testimony concerning whether the PTO considered NAV 95, this testimony was directed to alleged similar technology in the Endrijonas reference. (D.I. 810 at 10 (citing Tr. at 2172:6-2175:13).) Moreover, Dr. Spafford consistently testified that he relied upon the functionality of the NAV 95 product itself, as shown by the user guide, software, and source code, and did not "conced[e]," as Finjan asserts, that each is a separate piece of prior art. (*Id.* (citing Tr. at 2088:24-2089:5, 2200:6-15).)

i. *Whether NAV 95 and HotJava are Prior Art*

The court finds that there was substantial evidence in the record for the jury to find that NAV 95 and HotJava were publicly used, known, or on sale in the United States prior to November 8, 1996. Despite Finjan's assertions to the contrary, Symantec presented evidence to corroborate witness testimony that NAV 95 was available in the United States. Specifically, in addition to presenting Mr. Nachenberg and Mr. Kennedy's testimony that NAV 95 was released in August of 1995, at the same time Windows 95 was released, Mr. Kennedy obtained a shrink-wrapped box of NAV 95 that contained the user manual, floppy disk, and warranty card, which was introduced into evidence as DX-4469 and DX-4649. (*Id.* at 11 (citing Tr. at 1888:21-1889:18).) Mr. Kennedy also obtained the source code for NAV 95 (DX-4470) and verified that the dates and binary copies of the source code correspond to the dates and binary codes on the floppy disks in DX-4469. (*Id.* (citing Tr. at 1890:13-1891:13).) Moreover, consistent with the testimony presented, the user manual and executable program contain copyright dates of 1995 and indicate that the product was available in the United States,[9] and the source code contains data modified stamps prior to August 1995. (*Id.* (citing DX-4649-4, -78, -156; DX-4470, p. 1, 95, 127; SYMDX9-24).) Mr. Touboul, the inventor of the asserted patents, also testified that he was familiar with Norton Antivirus products in 1995-1996. (*Id.* (Tr. at 591:24-592:9, 631:15-18).) Thus, it is clear that there was evidence in the record corroborating the "interested" testimony of Mr. Nechenberg and Mr. Kennedy.

The testimony regarding the public availability of HotJava in the United States was likewise corroborated by documentary evidence. Specifically, an Oracle representative, Mr. Nisewanger, testified that the pre-beta 1 release of the HotJava browser and the source code on which Dr. Spafford relied were released to developers in the United States in May 1996. (*Id.*

[9] As the court explained in Section III.A.1.a.i, in connection with Finjan's copyright hearsay arguments, the court agrees with Symantec that Finjan failed to object to the copyright date as hearsay at trial and, regardless, Symantec presented evidence in addition to the copyright date to support its argument.

(citing Tr. at 2063:6-23, 2068:5-2070:20; DX-4140).) In addition, contrary to Finjan's assertion that Dr. Spafford "confirmed that pre-beta release means 'possibly intended only for internal consumption or a very select audience,'" he testified that a pre-beta release "is generally one that has most of the flaws worked out, most of the implementation in place and is shipped to the users to provide feedback prior to the final release." (*Id.* at 12 (citing Tr. at 2185:3-2186:25; *Oracle Corp. v. Parallel Networks, LLP*, 588 F. Supp. 2d 549, 570 (D. Del. 2008) (relying upon a beta release of the alleged prior art software)).) Thus, in view of the foregoing, the court concludes that the jury could have relied on substantial evidence in the record demonstrating that both NAV 95 and HotJava were available in the United States before November 8, 1996.

ii. *Whether NAV95 Discloses the Disputed Elements of the Asserted Claims of the '962 Patent*

The court further finds that Symantec presented substantial evidence through Dr. Spafford's testimony that NAV 95 disclosed the four claim elements. With regard to the "plurality of subsystems" element, Dr. Spafford testified that NAV 95 monitored the file subsystem and the I/O subsystem of the operating system. (*Id.* (citing Tr. at 2100:2-2140:15).) The NAV 95 user manual and software demonstrate that the product monitored multiple subsystems, and the NAV 95 source code also described a "file system event manager" and a separate "I/O system event manager." (*Id.* (citing DX-4649; DX-4469; SYMDX9-27, -28, -33; DX-4470, p. 18, 95, 127).) A Microsoft book also described the "block I/O subsystem" in Windows 95. (*Id.* (citing DX-4336-17).) Thus, the jury could conclude that Dr. Vigna's opinion was inconsistent with this evidence, including the Windows 95 book, as well as his own lecture notes, and the NAV 95 source code, which he did not review. (*Id.* (citing Tr. at 3030:3-6, 3123:24-3125:3; DX-4346-8).)

Regarding the "information pertaining to a Downloadable" element, Dr. Spafford explained that NAV 95 examined two types of information pertaining to a Downloadable: (1) it examined the request; and (2) it compared the identity of the program making the request against an exclusion list. (*Id.* at 12-13 (citing Tr. at 2110:15-2112:8, 2116:22-2117:5).) Symantec also notes that Finjan's expert, Dr. Medvidovic, testified that a request made by a Downloadable is information pertaining to the Downloadable and that, during claim construction, Finjan conceded that the identity of a Downloadable is information pertaining to that Downloadable. (*Id.* at 13 (citing Tr. at 1002:3-21; D.I. 182 at 14).) Moreover, Symantec notes that Dr. Spafford did not testify that NAV 95 would simply "avoid[] examining certain files" (D.I. 791 at 14), but instead opined that it would monitor for a request, compare information about the Downloadable to the policy, and then perform a predetermined response based on information pertaining to the Downloadable. (D.I. 810 at 13 (citing Tr. at 2112:19-2113:14).) Further, and with respect to Finjan's citing to Websense's non-infringement expert on this issue, Symantec notes that Finjan did not accuse Websense of infringing the '962 Patent and, therefore, Websense's expert did not address any term related to the claims of the '962 Patent that NAV 95 was found to invalidate. (*Id.* at n.5.)

In response to Finjan's assertion that there was no motivation to combine NAV 95 and HotJava, Dr. Spafford testified that there would have been such motivation based on the principle of defense in depth. (*Id.* (citing Tr. at 2135:23-2136:19).) Dr. Spafford also demonstrated how the products could be used on the same computer and how the combination would monitor multiple subsystems of the operating system, including the network subsystem. (*Id.* (citing Tr. at 2129:4-2131:12).) In its briefing, Finjan maintains that Dr. Spafford's testimony was conclusory and failed to establish a particularized motivation in the art.

Specifically, Finjan cites to such testimony as Dr. Spafford's statement that, "you would run extra programs, to make sure you were defended against everything," in support. (D.I. 791 at 8 (citing Tr. at 2136:1-3).) However, Dr. Spafford testified in detail that defense in depth was a concept well known in the prior art and in the security community at least since 1986, when he referenced the concept in his book. *See* Tr. at 2091:4-2092:6. Consequently, the court is not persuaded by Finjan's argument that Dr. Spafford's testimony on this point can be characterized as conclusory or that there was insufficient evidence in the record. Rather, the court finds that the jury could have concluded that Dr. Spafford's opinion as to motivation in the art was grounded in the concerns reflected in the defense in depth concept.

Finally, the court also agrees with Symantec that it presented substantial evidence that NAV 95 added information pertaining to the Downloadable to a suspicious Downloadables database. (D.I. 810 at 13.) Specifically, Dr. Spafford testified that NAV 95 would add information about the Downloadable to an "activity log," which was a database of suspicious Downloadables. (*Id.* at 14 (citing Tr. at 2118:14-2120:8; DX-4649-83, -84; SYMDX9-39).) Finjan contends that Claim 55 is not met because NAV 95 "has nothing resembling the claimed 'Downloadable Database' other than an 'activity log,' which is just a simple text file," and that, as a matter of claim construction, "such a simple text file is not a database." (D.I. 791 at 8 (citing *MySpace, Inc. v. Graphon Corp.*, 756 F. Supp. 2d 1218, 1232 (N.D. Cal. 2010), *aff'd*, 672 F.3d 1250 (Fed. Cir. 2012) (construing database as a "collection of data with a given structure that can be stored and retrieved.")).)

However, Dr. Spafford testified that, in his opinion, this claim limitation was met because, for reasons not fully recited here, he was able to "configure the activity log to indicate what suspicious activities [he] wanted to log, or to store in the database, along with the name of the file to be created, the database, and how large it could be." *See* Tr. at 2119:9-16. To this end, files were "added by the predetermined responsive action, setting the log, and indicating what it is ahead of time that you wanted to store, it's information pertaining to the Downloadable because it's the name of the file, its location, what it tried to do and when it happened." *Id.* at 2119:24-2120:8. Thus, Dr. Spafford concluded that because the files "are in the suspicious Downloadables database," Claim 55 is invalid. *See id.* Here, database was not construed during claim construction and Dr. Spafford provided his opinion based on his review of the claims and of NAV 95.

While Finjan is correct that Dr. Vigna presented a different opinion as to whether NAV 95 disclosed the claim elements, it was within the province of the jury to assess the credibility of each opinion and, ultimately, to accept Dr. Spafford's conclusions. In consideration of the evidence presented above, the court finds that the jury could have reasonably found substantial evidence in the record to support that conclusion.

2. Anticipation

At trial, Sophos and Websense asserted an anticipation invalidity defense against the '194 and '962 Patents based on the prior art reference SWEEP-InterCheck. The court discusses the parties' arguments, the evidence presented at trial, and the jury verdict below and finds, for the reasons that follow, that the jury's finding of invalidity was supported by substantial evidence.

Finjan asserts that the record is "devoid of evidence" that the specific prior art reference on which Sophos and Websense rely—version 2.72 of Sweep and version 2.11 of InterCheck—was available in the United States as a combined product before November 8, 1996, if ever. (D.I. 821 at 2.) Instead, Finjan maintains that Sophos presented the jury with "an assortment of generalized evidence, unrelated to the specific combination actually asserted as prior art" and included "many plainly erroneous and internally inconsistent dates." (*Id.* at 2-3.) For instance, Finjan notes that Sophos' invalidity expert, Mr. Klausner, claimed that disks not created until at least 1996 had been sold in 1995, that a CD ROM created in 2011 contained prior art, and that files dated 1995 and 1996 were not created until this litigation. (*Id.* at 3.) Finjan also asserts that Sophos failed to establish that the manuals on which it relied were enabled[10] and did not provide a "legally sufficient basis for combining the disparate versions, materials[,] and even a third-party hardware component that it presented to the jury as a purported single anticipating prior art reference." (*Id.*) Finally, Finjan contends that Sophos did not establish that Sweep-InterCheck disclosed the claim limitations: (1) checking Downloadables with a server serving as a "gateway" to the client; (2) using a security policy; (3) a server preventing execution of files; and (4) processing JavaScript and Visual Basic Script. (*Id.*) In light of the evidence presented at trial, the court disagrees and finds that the jury's verdict of invalidity was, in fact, based on substantial evidence.

The court disagrees and concludes that Sophos did present evidence sufficient to support the jury's verdict of invalidity as to the patents-in-suit, including: (1) testimony from Sophos founder and inventor, Dr. Jan Hruska; (2) testimony from Sophos software engineer Tim Twaits; (3) expert testimony from David Klausner demonstrating that every limitation of the asserted claims were present in SWEEP-InterCheck; (4) an in-court demonstration proving that SWEEP-InterCheck performed every limitation of the asserted claims; and (5) documentary evidence including a sales contract, source code, and product manuals. In fact, the court finds that the testimony and corroborating evidence could have led the jury to reasonably conclude that

[10] *See supra* note 7. Again, the court will not address the issue of enablement, as Finjan represented before trial that it would not be introducing enablement testimony with respect to any of the alleged pieces of prior art.

SWEEP-InterCheck was available in the United States at least as early as August 5, 1995. The court addresses each of Finjan's JMOL arguments below.

i. *Whether Substantial Evidence Demonstrated that SWEEP-InterCheck Was Available in the United States Before November 8, 1996*

Finjan maintains that Sophos did not provide relevant evidence of the availability of a combination of Sweep 2.72 and InterCheck 2.11 as a combined product in the United States before the November 8, 1996 priority date. Specifically, Finjan argues that Sophos relied on several purported versions of source code for Sweep and InterCheck and never entered into evidence an actual commercially available product corresponding to Sweep 2.72, InterCheck 2.11, or any other version of those software products, "let alone a combination of the two programs in a single product." (D.I. 790 at 4.) Finjan notes as contrast that Symantec entered into evidence a purported box copy of the NAV 95 product that it alleged to be prior art. (*Id.*) Here, Finjan states that Sophos showed the jury a demonstrative form of a CD ROM purporting to contain Sweep and InterCheck code, but that the disk was not created until 2011.

In addition, Finjan contends that Sophos failed to establish that the combination product was ever sold in the United States because: (1) Sophos relied on an unsigned August 1995 contract of Sophos' alleged sale of unidentified versions of Sweep and InterCheck that were for a Macintosh version of InterCheck, making it irrelevant here; (2) Dr. Hruska relied on this unexecuted contract to form his belief that Sweep-InterCheck was on sale in the United States before the priority date, which was uncorroborated and does not rise to clear and convincing evidence; (3) the October 2, 1994 source code comment on which Mr. Klausner relied to show U.S. availability of Sweep version 2.66 is inadmissible hearsay[11]; and (4) the testimony of

[11] Finjan also asserts that Sophos presented "evidence riddled with inconsistencies and errors regarding dates associated with InterCheck and Sweep. (D.I. 790 at 7.) For instance, Finjan notes that Mr. Klausner's

Sophos employees, Dr. Hruska and Mr. Timothy Twaits, did not establish availability. (*Id.* at 4-7.)

Based on the evidence presented at trial, the court finds substantial evidence to support the jury verdict. Specifically, the court agrees with Sophos that Finjan mischaracterizes Dr. Hruska's testimony in its Opening Brief in Support JMOL, stating that he "testified that he 'believed' SWEEP-InterCheck was on sale in the United States before the priority date, but did not provide any testimony beyond the insufficient disclosure of the document." (D.I. 812 at 4 (citing D.I. 791 at 5; DX-9047).) Rather, Dr. Hruska testified that SWEEP-InterCheck was sold in the United States before November 1995 and that he was personally involved in selling products to the World Bank in Washington, D.C. in 1995. (*Id.*) Dr. Hruska also authenticated, laid foundation for, and testified about the 1995 contract. (*Id.* (citing Tr. at 2354:15-2355:12).) Sophos sought to demonstrate this availability via Dr. Hruska's testimony that SWEEP-InterCheck for Windows 95 was sold in the United States by 1995, which was corroborated by the fact that one of Sophos' U.S. distributors was listed in the user manual for that product. (*Id.* (citing Tr. at 2340:3-17; DX-8406).)

In addition, Sophos introduced evidence to demonstrate its claim of priority by showing a comment in the SWEEP-InterCheck source code adding certain functionality to the product in

demonstrative exhibits had modification dates ranging from 1990 to 1995, "calling into serious question the verifiability of other times and data relied upon by Sophos." (*Id.*) In addition, Finjan asserts that Mr. Klausner told the jury that he was relying on software found in floppy disks he showed the jury that he claimed were shipped in 1995, when they were, in fact, dated 29/07/96, which was "long after Mr. Klausner claimed they were available." (*Id.* at 7-8.) Finjan also argues that: the SWEEPNT version 2.87 purportedly on the disks was not the Sweep 2.72 and InterCheck version 2.11 upon which Mr. Klausner relied; the CD ROMs that were to contain the purported prior art have a "copyright and build date as late as 2011"; and Mr. Klausner used various versions of InterCheck, raising "significant doubt regarding the accuracy of the release dates of these versions of InterCheck because the release dates for software versions are not chronologically linked to the version number." (*Id.*) In light of these inconsistencies, Finjan maintains that Sophos did not present clear and convincing evidence of invalidity. (*Id.* at 8.) The court discusses these assertions in its disposition of Finjan's Motion for a New Trial *infra*. *See infra* Section III.D.

October 1994 "for a US customer."[12] (*Id.* (citing SOP DX4-5, citing DX-8418).) While Finjan argues that this source code comment is inadmissible hearsay, Sophos correctly notes that Finjan did not raise this objection at trial. (*Id.*) Moreover, even if Finjan could introduce an objection to this evidence at this stage, its reliance on *Hilgraeve* to support its proposition is misplaced, as detailed above. Specifically, unlike in that case, where the defendant could not demonstrate that certain references were prior art because the only evidence offered was conclusory declarations, copyright labels, and other date stamps, here, Sophos has offered: testimony of the inventor of the prior art reference who established sales of it prior to the critical date; the World Bank contract; dated source code; dated manuals; and Mr. Twait's testimony about the InterCheck product development. (*Id.* at 5 (citing *Hilgraeve*, 271 F. Supp. 2d at 975 ("it is noteworthy that Defendant has failed to produce contemporaneous shipping records or sales receipts to prove that SAM 1.3 was actually shipped and sold to customers prior to February 1990")); Tr. at 2340:3-17, 2354:15-2355:12, 2351:9-12; DX-9047; DX-8406).)

Finjan's argument that SWEEP-InterCheck is not prior art because the demonstrative programs had multiple modification dates, and are, therefore, unreliable, also fails to prove a lack of substantial evidence. Indeed, Finjan's assertion that there is "significant doubt" as to the release dates of the versions of InterCheck presented at trial, is supported by a citation to demonstrative exhibit, SOP DX4-2. (*Id.* at 6.) Dr. Hruska and Mr. Twaits testified about how Sophos maintained its products and revision histories and each explained the use and procedures for the dates of various versions of Sophos products. (*Id.* (citing Tr. at 2331:3-2332:15, 2348:9-18, 2351:9-12).) If the jury found this testimony credible, as it appears to have done in this case, it could reasonably have found that the dates were not inconsistent as Finjan alleges and that the

[12] Finjan asserts that, "to the extent the comment in the source code is offered for the truth regarding the date SWEEP became publicly available, it is inadmissible hearsay." (D.I. 790 at 6 (citing *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 974 n.4 (E.D. Mich. 2003)).)

SWEEP-InterCheck release date was proven clearly and convincingly. Notably, Finjan did not cross-examine Dr. Hruska or Mr. Twaits on their explanations. Having failed to establish through cross-examination any dispute as to the veracity of the dates on each and every release of the Sophos software, it cannot now argue that Sophos' evidence is deficient as claimed. (*Id.* (citing *Symbol Techs., Inc. v. Opticon, Inc.*, 935 F.2d 1569, 1576 (Fed. Cir. 1991) (concluding that a party who chooses not to cross-examine a witness on an issue cannot later "recoup for its failed litigation strategy"); *GNB Battery Techs., Inc. v. Exide Corp.*, 876 F. Supp. 582, 604 (D. Del. Nov. 12, 2009) (same); *Linear Tech. Corp. v. Monolithic Power Sys., Inc.*, 2009 WL 3805567, at *6 (D. Del. Nov. 12, 2009) (same)).)

Finjan's criticism of Mr. Klausner's reliance on a floppy disk is also unavailing. Specifically, and as Sophos notes in its brief in opposition to JMOL, Mr. Klausner used the floppy disk to demonstrate how SWEEP-InterCheck met the claim limitation "computer readable storage medium," rather than to show when SWEEP-InterCheck was released. (*Id.* (citing Tr. at 2467:17-25).) Indeed, Mr. Klausner testified specifically as to which release he used in his invalidity analysis, stating that he relied on SWEEP version 2.72 and InterCheck version 2.11, as well as on InterCheck versions 2.01 and 2.10, which were earlier versions of the program incorporated into version 2.11. (*Id.* at 5-6, n.6 (citing Tr. at 2488:8-11, 2413:1-2476:6).)

In view of the foregoing, the court finds that Sophos presented substantial evidence on which the jury could have reasonably relied in reaching its conclusion that SWEEP-InterCheck was available in the United States before the November 1996 priority date of the patents-in-suit.

ii. *Whether Sophos Improperly Relied on Multiple References to Demonstrate Invalidity by Anticipation*

Finjan further asserts that Sophos: (1) "improperly argued anticipation based on a combination of references," including "a combination of documents, versions of source code[,] and executable files"; and (2) presented a "flawed" anticipation defense because it relied on a "third-party 'network interface card'" to satisfy the claim limitation "interface for receiving an incoming Downloadable addressed to a client" in Claim 32. (D.I. 790 at 9, 11.) In response to Finjan's first argument, Sophos maintains that it used a single product, SWEEP-InterCheck, to prove anticipation. Specifically, Sophos notes that its citations to source code were to a single version of SWEEP (version 2.72) and a single version of InterCheck (version 2.11), which were sold together as a single software product. (D.I. 812 at 7 (citing Tr. at 2419:2-11, 2431:24-2432:7, 2435:4-19).) Mr. Klausner also testified that he used these versions of the software in the SWEEP-InterCheck demonstration that he displayed at trial and confirmed this point during cross-examination.[13] (*Id.* (citing Tr. at 2420:18-2424:15, 2446:6-2448:22, 2487:16-2488:11, 2489:22-2490:21).) Mr. Klausner even testified that he did not perform an obviousness analysis because the software was sold as a single product. (*Id.* at 8 (citing Tr. at 2491:11-14).)

Sophos further challenges Finjan's "multiple references" argument, by detailing that the user manuals and source code are not independent prior art references, but rather are proof of how the SWEEP-InterCheck product operated and functioned at the relevant time. (*Id.* (citing 2383:4-9, 2415:2-2416:5).) As the Federal Circuit clarified in *Enzo Biochem, Inc. v. Gen-Probe, Inc.*, the combination of a product with a contemporaneous manual that ships with the device is a single reference for anticipation. (*Id.* (citing 424 F.3d 1276, 1285 (Fed. Cir. 2005) (using the product and "accompanying instructions" in an anticipation analysis)).) The court finds the Federal Circuit's opinion in *Enzo Biochem, Inc. v. Gen-Probe, Inc.*, to be more analogous to the instant case, than *Kyocera Wireless Corp. v. ITC*, which Finjan cites in support of its contention

[13] Sophos details that the evidence on which Mr. Klausner relied to establish the functionalities of SWEEP-InterCheck consisted of the source code for SWEEP version 2.72, InterCheck version 2.01, and InterCheck version 2.11, while his demonstration of the working product was confined to SWEEP version 2.72 running on Windows NT 3.51 and InterCheck version 2.11 running on a Windows 95 client computer. (D.I. 812 at 7 n.4 (citing Tr. at 2420:12-2426:15, 2384:19-2388:25).)

that Sophos relied on distinct pieces of prior art that cannot be characterized as a single product. *See* 545 F.3d 1340, 1351-52 (Fed. Cir. 2008) (concluding that a collection of technical specifications collectively known as the GSM standard, written by several different authors over several years and each constituting a separate document in its own right, do not function as a single prior art reference). Here, as noted above, Mr. Klausner relied on the user manuals and source code simply to demonstrate and support how SWEEP-InterCheck functioned at the time, not as distinct references. (D.I. 812 at 8 (citing Tr. at 2340:3-17, 2354:15-2355:12, 2351:9-12; DX-9047; DX-8406).)

Moreover, and in response to Finjan's assertion that it improperly relied on a "third-party 'network interface card,'" Sophos makes several arguments. First, Sophos argues that Claim 32 is, in fact, directed to a "system for execution by a server that serves as a gateway to a client," and, therefore, any component that is part of the "server that serves as a gateway to a client" is necessarily part of the claimed system. (*Id.* (citing '962 Patent at Claim 32).) Second, Sophos details that Mr. Klausner testified that the network card was an "example" of the claimed interface, and that the interface could be in hardware or software. (*Id.* (citing Tr. at 2440:9-241:15).) To this end, Sophos asserts that it "proved in multiple ways that SWEEP-InterCheck discloses this claim limitation." Third, Sophos contends that, in any event, a network interface is inherent in SWEEP-InterCheck. (*Id.* at 8-9 (citing *Schering Corp. v. Geneva Pharmaceuticals*, 339 F.3d 1373, 1377 (Fed. Cir. 2003) ("A prior art reference may anticipate without disclosing a feature of the claimed invention if that missing characteristic is necessarily present, or inherent, in a single anticipating reference.")).) Specifically, Sophos notes that, just as a computer is necessary to run SWEEP-InterCheck, a network interface is necessary to "receiv[e] an incoming Downloadable addressed to a client." (*Id.* at 9 (citation omitted).) Thus, because SWEEP-

InterCheck was "indisputably able to receive incoming [D]ownloadables," which the jury saw during Mr. Klausner's demonstration, Sophos asserts that it is clear that SWEEP-InterCheck satisfies the "interface" limitation of Claim 32. (*Id.*)

The court agrees with Sophos that, because Claim 32 is directed to "system for execution by a server that serves as a gateway," a component that is a part of the "server that serves as a gateway to a client" is a necessary part of that claimed system. Indeed, as Sophos details, as SWEEP-InterCheck receives incoming Downloadables, a functionality that the jury observed, it is clear that a network interface would be necessary to receive that Downloadable. The network interface card that Mr. Klausner referenced served as an example of the claimed interface and he concluded that SWEEP-InterCheck disclosed this claim.[14] Thus, the court finds that there was sufficient evidence in the record for the jury to find, accepting Mr. Klausner's testimony as credible, that Claim 32 was disclosed in SWEEP-InterCheck.

iii. *Whether SWEEP-InterCheck Discloses Each Limitation of the Asserted Claims of the '194 Patent*

In addition to the foregoing, Finjan also contends that Sophos failed to demonstrate that SWEEP-InterCheck discloses each limitation of the asserted claims. Specifically, Finjan asserts, with respect to the '194 Patent, that SWEEP-InterCheck: (1) did not disclose a server, acting as a gateway to a client, that checks incoming Downloadables before they are delivered to the client, because, as Dr. Vigna testified, it did not have a gateway[15] and, instead, allowed for delivery to a

[14] Specifically, Mr. Klausner testified, in response to the question "[h]ow do you find that limitation to be met by the SWEEP/InterCheck product," that he found this limitation:

> [b]y an example of an interface. I am holding up an interface. This is inside the machine, in the back. And you plug the Internet into that hole. You plug the cable into that hole. And this is called officially a network interface card. . . . This is SOP DX-7.

Tr. at 2440:9-25. Mr. Klausner also noted that SOP DX-7 is a 1995 era interface card and, in his opinion, meets the claim limitation. *Id.* at 2441:1-5.

[15] Finajn also argues that Sophos conceded that SWEEP-InterCheck did not have a gateway via the testimony of Mr. Twaits, who confirmed that a Downloadable file can be downloaded from the Internet onto a client computer without being scanned by the SWEEP server. (D.I. 790 at 12 (citing Tr. at 2395:18-2400:2).) Moreover,

client before the server checked the Downloadable (D.I. 790 at 12); (2) did not satisfy the step of "comparing, by the server, Downloadable security profile data pertaining to the Downloadable" because the comparison must be done by the server that serves as a gateway for the client (*id.* at 13 (citing Tr. at 3078:25-3079:13)); (3) did not meet the limitation that "the Downloadable security profile data includes a list of suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated" in all asserted claims or "decomposing the Downloadable into Downloadable security profile data," because these limitation require analysis of operations and SWEEP-InterCheck only provided traditional fingerprint/signature matching based detection, not protection based on the operations of a file (*id.* at 13-14 (citing Tr. at 3079:14-3080:21)); (4) did not perform the step of "preventing execution of the Downloadable by the client if the security policy has been violated, recited in all asserted claims" because the server must perform this step and in SWEEP-InterCheck, the server did not prevent downloading of a Downloadable or execution of a file by a client (*id.* at 14 (citing Tr. at 3080:22-3083:3)); (5) failed to invalidate Claims 10, 11, 33, 35, and 36, which recited evaluating Downloadables with either JavaScript or Visual Basic Code because Sophos' invalidity expert conceded that SWEEP-InterCheck was not capable of examining such code in a Downloadable for malware (*id.* (citing Tr. at 2473:3-17, 2499:4-15, 3093:4-6)); and (6) did not satisfy the limitation that "the Downloadable security profile data includes a list of suspicious computer operations that may be attempted by the Downloadable" and Mr. Klausner did not reference it in his testimony (*id.* at 14-15).

However, in view of the record before it, the court finds that Sophos presented substantial evidence via Mr. Klausner's testimony, that SWEEP-InterCheck did, in fact, disclose each

Finjan cites to Mr. Twaits testimony as supporting the proposition that a file recognized by the client as a known file would be executed without any call to the SWEEP-server program. (*Id.* (citing Tr. at 3160:13-3161:7).)

limitation of the asserted claims of the '194 Patent. *See Gomez v. Allegheny Health Servs., Inc.*, 71 F.3d 1079, 1083 (3d Cir. 1995) (finding that a jury verdict should not be overturned where the record is not "critically deficient of the minimum quantum of evidence" to sustain it). First, and with regard to Finjan's assertion that SWEEP-InterCheck did not employ a "gateway," as required by the claims, Sophos cites to Mr. Twait's testimony to the contrary. Specifically, Mr. Twait testified that the Downloadable cannot be downloaded to a client computer without first being scanned by SWEEP and, further, that this scan acts as the required gateway. (D.I. 812 at 9 (citing Tr. at 2383:20-2388:1, 2396:14-2400:2).) In addition, Dr. Hruska testified that the Downloadable is not executable on a computer before being checked by the SWEEP server. (*Id.* (citing Tr. at 2372:14-16 (testifying "incorrect," in response to the question "[s]o it was already downloaded onto one of the computers before it hit the SWEEP server, correct?").) Indeed, Dr. Hruska explained that SWEEP-InterCheck would "make sure that you can't do anything with [the Downloadable] before it's been checked." (*Id.* at 9-10 (citing Tr. at 2400:1-2, 2399:7-2400:3).) In light of this testimony, it was reasonable for the jury to conclude that this claim limitation was met.

Second, and with regard to the "security policy" limitation, Sophos notes that Mr. Klausner "methodically established" that SWEEP-InterCheck discloses the use of a security policy. *See* Tr. at 2435:4-2436:6. In addition, Sophos maintains that Finjan inaccurately characterizes SWEEP-InterCheck as a signature-based technology, even though Finjan failed to establish this position at trial. Rather, Sophos presented evidence to demonstrate that SWEEP-InterCheck could detect unknown malware, such as polymorphic viruses and, further, that its security policy was used to determine whether malware, including such viruses, were present. (D.I. 812 at 10 (citing Tr. at 2349:5-2351:5, 2434:25-2435:19, 2456:14-24).) Moreover, regarding Finjan's claim that the "decomposing" element of Claim 66 is missing from Mr. Klausner's analysis, Mr. Klausner did testify as to the functionality of the decomposing element of Claim 66, which could reasonably establish that SWEEP-InterCheck used a security policy as required by the '194 Patent. Therefore, the court finds that if the jury agreed with Sophos' witnesses, it could have reasonably found that SWEEP-InterCheck disclosed the "security policy" limitation.

Third, Sophos also points to evidence in the record from which the jury could conclude that SWEEP-InterCheck disclosed the "prevent[s] the execution of the Downloadable" limitation. In making this argument, Sophos challenges Finjan's assertion that the server must prevent the execution of the downloadable, noting that nothing in the asserted claims requires the server to prevent such execution of the Downloadable. (*Id.*) Instead, the claims recite "preventing execution of the Downloadable by the client if the security policy has been violated," without specifying what must prevent the execution of the Downloadable. (*Id.* (citing '194 Patent at Claim 1).) And, regardless, Mr. Klausner testified that SWEEP-InterCheck prevented the client from executing the Downloadable by telling the client to block the file. (*Id.* at 10-11 (citing Tr. at 2435:4-2436:3, 2442:10-2443:3).)

Fourth, Sophos asserts that it proved, with unrebutted testimony and a demonstration, that SWEEP-InterCheck could process JavaScript and Visual Basic Downloadables. (*Id.* at 11 (citing Tr. at 2424:25-2426:9, 2443:11-2444:15).) Despite this evidence, Finjan contends that SWEEP-InterCheck did not possess this capability. However, as Mr. Klausner testified, the claims do not require that the Downloadable based on JavaScript or Visual Basic script contain the malware. (*Id.* (citing Tr. at 2473:3-17).) Thus, there was, in fact, evidence in the record supporting Sophos' position that SWEEP-InterCheck met this claim limitation.

Finally, and in response to Finjan's argument that Mr. Klausner "ignore[d]" a limitation in Claim 65, Sophos details that this allegedly "admitted" claim appears verbatim in several other claims, including Claim 1. (*Id.* (citing SOP DX4-36).) Indeed, Mr. Klausner testified repeatedly at trial that his analysis of identical claim limitations in different claims was the same. (*Id.* (citing Tr. at 2446:10-19).) Notably, Finjan does not contest that SWEEP-InterCheck practices the same limitation of Claim 1. (*Id.* (citing Tr. at 2432:8-2433:19).) Therefore, Finjan's assertion that Sophos, or Mr. Klausner specifically, somehow ignored this claim limitation is unpersuasive.

In view of the foregoing, the court finds that there was substantial evidence in the record, via Mr. Klausner and Dr. Hruska's testimony and Sophos' demonstration, that SWEEP-InterCheck meets each of the limitations of the asserted claims. The jury heard from both sides' experts and was within its right to determine which opinion was credible as to anticipation. The court will not, therefore, grant JMOL and overturn the jury's invalidity verdict with respect to the '194 Patent.

iv. *Whether SWEEP-InterCheck Discloses Each Limitation of the Asserted Claims of the '962 Patent*

Finally, Finjan asserts that Sophos failed to show that SWEEP-InterCheck disclosed the limitations of the asserted claims of the '962 Patent. In particular, Finjan argues that SWEEP-InterCheck: (1) did not "monitor[] substantially in parallel a plurality of subsystems of the operating system," because, as Dr. Vigna explained, it only monitors a single file subsystem, does not monitor other subsystems, and cannot be compensated for by the interrupt disk input/output operations and BIOS services (D.I. 790 at 15 (citing Tr. at 3094:21-3095:8)); (2) did not monitor files "during runtime," as required by the asserted claims because, as Mr. Klausner acknowledged, runtime "means during the execution of the program," such that all actions that take place before or after a program is executed (*id.* at 16 (citing Tr. at 2453:17-2454:18)); (3) did not perform the step of "comparing information pertaining to the Downloadable against a predetermined security policy, because this limitation requires looking at the Downloadable and it only looked at information about the "target" of a Downloadable's operation, not the Downloadable program trying to execute the target (*id.*); and (4) failed to disclose the step of monitoring a "network system," because its function was limited to monitoring network drives, which are just part of a file that are remotely accessed and did not monitor network subsystems of an operating system (*id.* at 17 (citing Tr. at 3101:1-3102:5)).

In consideration of the evidence detailed below, the court disagrees and finds that the jury's invalidity verdict as to the '962 Patent is supported by substantial evidence. First, Sophos argues that it presented evidence that SWEEP-InterCheck monitored a plurality of subsystems. Specifically, Mr. Klausner testified about the various subsystem calls for the file systems and disk access, referencing InterCheck source code to explain how the subsystems are handled. (D.I. 812 at 12 (citing Tr. at 2451:24-2453:2).) In addition, Sophos notes that the Dr. Vigna testimony to which Finjan cites to support its contention that SWEEP-InterCheck did not monitor a plurality of subsystems, includes Dr. Vigna's opinion about NAV 95, an unrelated product. (*Id.* (citing 790 at 16).) In its Reply, Finjan clarifies its argument and disagrees with Mr. Klausner's testimony that SWEEP-InterCheck was capable of monitoring multiple subsystems because it monitored "file system," "disk access," and "disk input/output" interrupts. (D.I. 820 at 7 (citing D.I. 812 at 12).)

In contrast, Finjan maintains that Mr. Klausner did not demonstrate monitoring of a plurality of subsystems because each of the "interrupts" Mr. Klausner identified are "file operations contained in a File System, a single subsystem of the Operating System," such that

Sophos did not rebut its showing that "monitoring disk access and disk input/output simply means writing and reading files within a single subsystem and not multiple subsystems, as required by the asserted claims." (*Id.*) Finjan also argues that Sophos did not rebut Finjan's "explanation that BIOS (Basic Input/Output System) operations are not within one of the subsystems of the operating system because they are performed when a computer is first booted up, before an operating system is loaded and, thus, cannot satisfy the limitation of monitoring an operating system." (*Id.*) Importantly, however, Mr. Klausner's testimony included his opinion, based on his assessment of the product and its source code, that the interrupts were "different than files" and were, instead, "another subsystem." *See, e.g.*, Tr. at 2450:14-2. While Dr. Vigna came to a different conclusion and Finjan disagrees with Mr. Klausner's analysis, the jury was entitled to weigh the credibility of both opinions and agree with Mr. Klausner that SWEEP-InterCheck monitored a plurality of subsystems, satisfying this claim limitation.

In addition, the court finds that Sophos did introduce evidence that SWEEP-InterCheck monitored files during "runtime." Specifically, Mr. Klausner detailed how SWEEP-InterCheck monitored files during runtime and referenced source code, a demonstrative showing runtime monitoring, and other evidence in support. For instance, Mr. Klausner testified as to examples of opening, closing, and writing a file to establish this claim and counter Dr. Vigna's testimony that SWEEP-InterCheck only provided access scanning. (D.I. 812 at 12 (citing Tr. at 2453:17-2454:18).) Again, the court finds that both sides presented the jury with evidence as to whether SWEEP-InterCheck met the runtime claim limitation and that it was reasonable for the jury to find substantial support for Mr. Klausner's opinion.

Similarly, Sophos also presented evidence through Mr. Klausner's testimony that SWEEP-InterCheck disclosed a comparator and response engine, contrary to Finjan's assertion that it did not compare information pertaining to the Downloadable. (*Id.* (citing D.I. 790 at 12-16).) In particular, and as Sophos notes, a similar element in the '194 Patent requires comparison against a security policy and Finjan does not dispute that SWEEP-InterCheck practiced that element. Regardless, Mr. Klausner cited and displayed source code that compared information pertaining to a Downloadable (e.g., through control.asm) against a predetermined security policy (e.g., abort_call). (*Id.* (citing Tr. at 2456:14-2458:3).) In addition, Mr. Klausner described how SWEEP-InterCheck's comparator and response engine would compare the Downloadable against the predetermined policy to recognize whether the Downloadable contained any malware. (*Id.* at 13 (citing Tr. at 2456:10-2458:3).) Thus, the court finds that the jury had evidence sufficient to reasonably reject Finjan's claims that the comparator and response engine did not exist in SWEEP-InterCheck.

Finally, with respect to the claimed elements, Sophos also presented substantial evidence from which the jury could find that SWEEP-InterCheck monitors a network system. Specifically, Mr. Klausner discussed how SWEEP-InterCheck checked multiple subsystems, including network systems, and identified the various systems being monitored. (*Id.* (citing Tr. at 2469:18-2471:18; DX-8419; DX-8421).) Mr. Klausner explained that these subsystems included a file system, network system, process system, and memory systems. (*Id.*) Thus, despite Dr. Vigna's testimony to the contrary that SWEEP-InterCheck was limited to monitoring network drives, which are just part of the file system that are remotely accessed—not a network subsystem of an operating system—Mr. Klausner presented a different conclusion with which the jury could reasonably agree.

With regard to the jury's agreement with Mr. Klausner's opinion that SWEEP-InterCheck anticipated the asserted claims of the '962 Patent, it was within the province of the jury to assess the credibility of each side's experts and draw reasonable conclusions. As Sophos points out in its briefing, Dr. Vigna testified that he did not review the SWEEP-InterCheck source code in forming his opinion. (D.I. 812 at 13 (citing Tr. at 471:21-472:1, 724:4-5, 3143:3-3144:13).) Sophos also notes that even one of Finjan's experts referred to the source code as "the DNA of the system in question," and that, despite the importance of source code, Dr. Vigna did not review a "line of it" in conducting his analysis, because he did not sign the Protective Order between the parties (*Id.* at 14 (citing Tr. at 471:21-472:1, 724:4-5, 3143:3-3144:13).) While Dr. Vigna did testify generally on direct examination that he reviewed the binary code to determine how the products functioned, the court prevented him from elaborating during redirect on this analysis.[16] Indeed, as Sophos notes, Dr. Vigna was the only expert Finjan offered to challenge the Sophos' validity defense and Dr. Vigna opined on SWEEP-InterCheck for less than ten pages of his two-hundred and fifty page expert report. Thus, for the reasons outlined above, the court concludes that it would have been reasonable for the jury to find the patents-in-suit invalid in light of SWEEP-InterCheck based on the substantial evidence in the record.

The court also notes that, as Sophos correctly asserts in its Brief in Opposition to Finjan's JMOL motion, the jury's invalidity verdict is further supported by the prior art asserted by the other defendants. In fact, the jury verdict form made this point clear in asking: "Do you find that any of the Defendants have proven by clear and convincing evidence that any of the asserted claims [of each asserted patent] are invalid because they are anticipated by prior art?" (*Id.* at 15

[16] Specifically, the court engaged in the following discussion with counsel at sidebar:

> Finjan's Counsel: Now, you mentioned binary code in connection with Sweep/InterCheck, and you thought this was a better source of material. Why is that?
>
> The Court: Let me see counsel. (The following discussion took place at sidebar.) It's not my job to judge this witness' credibility, but I am not going to let him confuse this jury with a discussion about binary code. No expert in this case has talked about binary code, including this gentleman on his direct testimony.

Tr. at 3159:15-3160:1. The court discusses its rationale in precluding Dr. Vigna from testifying in greater detail as to his review of the binary code *infra*. *See infra* Section III.D.

(citing D.I. 746 at 4).) The jury's verdict of invalidity based on anticipation and obviousness further demonstrates that the jury considered all the prior art, because Sophos did not make an obviousness argument based on SWEEP-InterCheck. Therefore, it appears that the jury must have relied on other prior art to find the patent obvious. While Finjan overlooks this point in its briefing, it does support the jury verdict in this case.

B. Infringement

Finjan also moves for judgment as a matter of law on the issue of infringement. The court will address infringement separately with respect to each defendant.

1. The Jury's Finding of Sophos' Noninfringement

Finjan moves for JMOL as to the jury's verdict that Sophos' HIPS Runtime products infringe the '962 Patent and that its Behavioral Genotype products infringe the '194 Patent. In support, Finjan asserts that Sophos did not challenge its evidence of infringement and, to the contrary, admitted during closing arguments that "Finjan filed patents, and the Patent Office granted patents, and those patent claims cover what we do." (D.I. 790 at 18 (citing Tr. at 3351:25-3352:2).) Finjan also cites to Sophos' closing argument statement that it had not "contended for a minute in this case that our products are not covered by their patents. They are. We did it first. That invalidates the patents." (*Id.* (citing Tr. at 3352:3-5).) Moreover, Finjan notes that its expert, Dr. Brumley, provided a detailed analysis demonstrating Sophos' infringement on a claim by claim basis and that Sophos did not challenge his infringement opinions, but, instead, focused its line of inquiry entirely on invalidity and which products and features were accused of infringement. (*Id.* (citing Tr. at 1091:22-1168:5, 1169:20-1176:1, 1195:8-1248:16, 1249:7-1273:8 (Brumley)).) Thus, Finjan argues that Sophos did not dispute infringement at trial and, as a result, the jury's verdict was unsupported by the evidence. Indeed, Finjan asserts that Sophos did not dispute infringement until its opposition to Finjan's first motion for JMOL, which is insufficient and serves merely as "unsupported attorney argument." (*Id.* at 18-19 (citing D.I. 761).)

Specifically, Finjan highlights that, with respect to the '194 Patent, Sophos' only non-infringement argument was that its Behavioral Genotype products do not operate as a "server that serves as a gateway to the client," but raised this argument only in its opposition to Finjan's Rule 50(a) JMOL. (*Id.* (citing D.I. 761).) Finjan contends that this unsupported attorney argument cannot overcome the dispositive evidence presented at trial—Dr. Brumley's unrebutted testimony that Sophos' products infringe the '194 Patent: (1) by serving as a gateway by scanning Downloadables before they can infect the client (*id.* (citing Tr. at 1196:15-1200:16 (Brumely))); (2) having the gateway implemented as a web proxy (*id.* (citing Tr. at 1242:6-1243:7 (Brumley); Ex. 30, JTX-292)); and (3) by their functionality, which is demonstrated through deposition and documents describing the products' functionality and pointing to various portions of Sophos' source code, which proves that the accused products do, in fact, have this functionality (*id.* (citing JTX-292; Ex. 1; Tr. at 1198:14-1200:16). Finjan argues that this testimony, coupled with Sophos' failure to challenge the Claim 66 infringement allegation, combines to render the jury verdict of noninfringement invalid. (*Id.*)

Likewise, Finjan maintains that Dr. Brumley's testimony and Sophos' failure to challenge his analysis or present a noninfringement argument on the '962 Patent, renders the jury's finding of noninfringement for that Patent unsupported by substantial evidence. Specifically, Finjan argues that it proved that Sophos' HIPS Runtime Products practice all limitations of the asserted claims of the '962 Patent through Dr. Brumley's testimony that: (1) Sophos' products perform the required monitoring (*id.* at 19 (citing Tr. at 1102:15-1104:4

(Brumley))); (2) Sophos installs hooks, which notify Sophos when files are modified (*id.* at 19-20 (citing Tr. at 1054:19-1055:12 (Brumley))); and (3) Microsoft does not support or recommend this approach (*id.* at 20 (citing Tr. at 1102:18-1103:7 (Brumley))). In addition, Finjan highlights that Sophos' invalidity expert, Mr. Klausner, also confirmed the way that hooking works as: "It's a way to—if there is a path through the operating system that says, do this, this, this, this, and this, hooking interrupts that path and says, by the way, take a detour right here so I can check something." (*Id.* (citing Tr. at 2456:4-8 (Klausner)).) To this end, Sophos installs these hooks for monitoring and then interrupts the processing of the requests and calls the SAV engine to do its analysis. (*Id.* (citing Tr. at 1102:18-1103:14 (Brumley)).)

Dr. Brumley testified that this, and the evidence in the record, indicates that "Sophos is doing the monitoring substantially in parallel for an event," a point that Finjan states Mr. Klausner confirmed by his testimony that Sophos' predecessor products do interrupt processing of the request. (*Id.* (citing Tr. at 1052:19-1055:7 (Brumley); Tr. at 2455:9-2456:13 (Klausner) (noting, in support of its argument that Sweep-InterCheck satisfies the "interrupting processing of the request" limitation, that Mr. Klausner testified: "we are interrupting a program that's running, that's trying to access some file in order to allow us to allow the checking of that file before we have that program continue to execute")).) Finjan further maintains that Mr. Twaits, a senior software development engineer at Sophos, likewise confirmed that its products perform the monitoring step. (*Id.* (citing Tr. at 1052:19-1055:7 (Twaits)).) Thus, Finjan urges the court to grant its motion for JMOL against Sophos and find the asserted claims of the '194 and '962 Patents infringed. (*Id.*)

In response, Sophos asserts that: (1) Finjan had the burden of proof on infringement and failed to meet that burden (D.I. 812 at 16); and (2) statements made by Sophos' counsel constitute attorney argument, not evidence, and, therefore, have no bearing on the jury's ultimate findings (*id.*). For the reasons set forth below, the court agrees and finds that the jury's finding of noninfringement with respect to Sophos' products was not against the weight of evidence.

Importantly, and as Sophos correctly notes, it was Finjan's burden to prove infringement of the '962 and '194 Patents, not Sophos' burden to prove noninfringement. Indeed, while Sophos did not present a separate noninfringement argument at trial, the record was not devoid of evidence supporting a conclusion of noninfringement and Sophos did challenge the credibility of Dr. Brumley's findings.

First, Sophos argues that both of its co-defendants, Symantec and Websense presented non-infringement arguments that were equally applicable to Sophos and, therefore, it would have been "unreasonable and inconsistent for the jury to find noninfringement for Symantec and Websense while finding [that it] infringed." (D.I. 812 at 16.) The court disagrees with Sophos that its co-defendants' infringement arguments were equally applicable to Sophos, because there is no evidence and no party argued that the defendants' products were similar or operated similarly. However, the court does agree that if the jury found that Dr. Brumley's opinions were not credible with respect to Symantec and Websense, as compared to the opinions asserted by the other defendants' witnesses, the jury could reasonably have applied its credibility assessment in evaluating Dr. Brumley's conclusion that Sophos infringed the asserted patents. *See Star Scientific, Inc. v. R.J. Reynolds Tobacco Co.*, 655 F.3d 1364, 1378 (Fed. Cir. 2011) (concluding that where expert testimony was needed to establish infringement, it was not unreasonable for the jury to discredit the testimony of the patentee's expert and find noninfringement).

Second, regarding the '962 Patent, the parties arguments focused on whether the Sophos' products practice at least the claim limitation "monitoring substantially in parallel a plurality of subsystems of the operating system." Sophos asserts and the court agrees, that it was reasonable for the jury to conclude that Finjan failed to prove infringement of this claim limitation through the evidence it adduced at trial. (*Id.* at 17.) Specifically, contrary to Finjan's assertion that Mr. Klausner's testimony demonstrates that the products practice this element through Sophos' installation of the hooks for monitoring in the SWEEP-InterCheck system, this testimony regarding invalidity did not necessarily show that the accused products also operate in the same way. (*Id.*)

In addition, Sophos notes that Finjan cites to only conclusory statements of Dr. Brumley that Sophos installed the hooks for monitoring and, thus, performed the limitation. Importantly, Dr. Brumley only stated that Sophos performed this monitoring step because Sophos interrupts the request and did not tie Sophos to the monitoring requirement. Sophos further asserts that Dr. Brumley did not sufficiently explain how Sophos met the claim limitation in Claims 12 and 21, requiring a plurality of the operating system interfaces operating substantially in parallel, such that, absent further analysis, which was not provided, the jury could have reasonably found that Finjan failed to establish infringement of these elements. (*Id.*) Finally, Sophos argues that Finjan failed to consider that the deposition testimony it relied on from Mr. Twaits described how the Sophos products "hook" the Microsoft operating system and, that by hooking into this operating system, it was Microsoft—not the Sophos products—that performed the "monitoring" element required by the claims. (*Id.* at 17 (citing Tr. at 1054:19-1055:12 (Twaits)).) In particular, Mr. Twaits' deposition testimony detailed how the "operating system [] will notify" Sophos when its registry values and keys have been modified. (*Id.* (citing Tr. at 1054:19-1055:2 (Twaits)).) Thus, because the operating system performs this monitoring, it was reasonable for jury to find that Sophos' accused products do not perform this limitation and, therefore, do not infringe.

Third, and with regard to the '194 Patent, the court likewise finds that the jury verdict of noninfringement was reasonable and was not against the weight of evidence. Specifically, Dr. Brumley relied on Virus Description Language ("VDL") to prove, at least in part, that the Sophos products practiced the "comparing" element of the '194 Patent that is present in each of the asserted claims. Importantly, on cross-examination, Sophos established that Dr. Brumley considered only a small portion of the source code available to him and questioned whether he sufficiently determined the functionality of the products at issue. Tr. at 1263:9-1264:2. Dr. Brumley also admitted on cross-examination that he did not know what VDL stood for until the trial began, which, Sophos maintains, demonstrated a gap in his understanding of the products. *See id.* at 1265:2-23, 1270:20-1272:11. In light of this cross-examination, the jury could have reasonably questioned the credibility and completeness of Dr. Brumley's analysis, entitling it to find that Finjan failed to carry its burden of proving infringement. Indeed, the Third Circuit has clarified that if, at the very least, the "record contains the minimum quantum of evidence" from which a jury could reasonably find a verdict, a JMOL motion should be denied. *See Keith v. Truck Stops Corp. of America*, 909 F.2d 547, 548 (3d Cir. 1986); *Price v. Delaware Dep't of Correction*, 40 F. Supp. 2d 544, 549-50 (D. Del. 1999).

In sum, the court agrees with Sophos that the jury's verdict was not against the weight of the evidence, as the jury could have reasonably found that Dr. Brumley's testimony did not conclusively establish infringement of each of the elements of the asserted claims of the patents-in-suit for the reasons detailed above.

Finally, the court finds that Sophos' closing argument statements, quoted above, do not undermine the jury's finding of noninfringement or establish that that verdict was not based on substantial evidence. It is well established that attorney argument does not constitute evidence. *See, e.g.*, *Gemtron Corp. v. Saint-Gobain Corp.*, 572 F.3d 1371, 1380 (Fed. Cir. 2009) (noting that "unsworn attorney argument . . . is not evidence"); *Johnston v. IVAC Corp.*, 885 F.2d 1574, 1581 (Fed. Cir. 1989) (concluding that attorney argument is no substitute for evidence). Thus, the jury should not have considered—and, evidently, did not consider—Sophos' counsel's statements to be evidence that Sophos' products infringe the patents-in-suit. Rather, the jury was tasked with assessing the evidence in the record in reaching its conclusion as to whether Finjan met its burden of proving infringement and, here, could have reasonably concluded that it did not.

In reaching its conclusion, the court rejects Finjan's contention that Sophos' counsel's closing argument statements should constitute an "admission" of infringement, necessitating JMOL. Specifically, Finjan argues that "Sophos took an unequivocal position at trial in admitting infringement, and used it to support an invalidity argument," and, therefore, "cannot now 'assume a contrary position simply because the decision in retrospect was a tactical mistake, or pherahps a candid but regrettable conclusion.'" (D.I. 820 at 9 (citing *Fleck v. KDI Sylvan Pools, Inc.*, 981 F.2d 107, 116-17 (3d Cir. 1992)).) First, and with regard to Finjan's assertion that Sophos made its statement "admitting infringement" to support its invalidity argument, attorney argument is not evidence and the jury properly did not consider the statement as evidence in reaching its verdict. Second, the court also disagrees with Finjan's position that Sophos' statements constituted an "unequivocal" admission, as required. *See Childs v. Franco*, 563 F. Supp. 290, 292 (E.D. Pa. 1983) ("If unequivocal, an admission of counsel during the course of trial is binding on the client."). Indeed, while an attorney's statement "may" constitute an admission, it must be unequivocal to result in a binding admission on the client. *See id.* Here, while Sophos did not present a noninfringement case, it was not Sophos' burden to do so and Sophos' questioned the credibility of Finjan's infringement expert on cross-examination. In addition, Sophos included infringement in the parties' Pretrial Order as an issue in dispute and the jury Verdict Form tasked the jury with determining whether Sophos' products infringed the patents-in-suit. Aside from Sophos' counsel's statements during his closing argument, there is no evidence in the record or in the litigation of this action, indicating that Sophos admitted to infringement. Thus, the court disagrees with Finjan's assertion that Sophos' counsel's statements constituted an admission requiring JMOL.

In view of the foregoing, the court concludes that the jury could have reasonably found that Finjan failed to carry its burden of demonstrating infringement by the required standard. *See Start Scientific, Inc. v. R.J. Reynolds Tobacco Co.*, 655 F.3d 1364, 13778 (Fed. Cir. 2011) (concluding that where expert testimony is needed to establish infringement, it is not unreasonable for a jury to discredit the testimony of the patentee's expert and find noninfringement). Therefore, the court finds that the jury verdict was not against the weight of the evidence and Finjan's JMOL with regard to Sophos' alleged infringement is denied.

2. Symantec & the Jury's Finding of Noninfringement

a. Noninfringement of the '194 Patent

Finjan maintains that the dispute between it and Symantec on the issue of infringement centered on whether, with respect to the '194 Patent, Symantec's Matrix accused technology meets the "a list of suspicious computer operations" limitation of the asserted claim. (D.I. 791 at 16.) Finjan asserts that, on this question of infringement, a reasonable jury could only find that

Symantec infringes the asserted claims of the '194 Patent. Specifically, Finjan argues that the jury verdict of noninfringement went against the weight of evidence because: (1) Symantec's expert, Dr. Maggs, conceded on cross-examination that Matrix's checking for "signature matches" encompasses "operations" within the meaning of claim; (2) Symantec's noninfringement arguments depended on an improper construction of the "list" limitation, making them "critically flawed"; and (3) Symantec's argument that Matrix does not generate "Downloadable security profile data," including "a list of suspicious computer operations," from the Downloadable code conflicts with the court's plain and ordinary meaning construction of the limitation. (D.I. 791 at 16-17.) In consideration of the evidence presented at trial and the relevant law, the court disagrees and concludes that the evidence presented was sufficient to support the jury's verdict of noninfringement.

As Symantec details in its Answering Brief in Opposition to JMOL, Symantec did, in fact, present substantial evidence that could reasonably support a finding of noninfringement. Specifically, Symantec, through the evidence it presented, sought to demonstrate that the accused Matrix technology does not infringe the '194 Patent, because it does not "compar[e], by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile includes a list of suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated." (D.I. 810 at 14 (citing Tr. at 1944:19-24, 1953:6-24; PTX-1, 10:11-15).) Indeed, Symantec presented fact and expert witnesses who testified that, rather than comparing a list of suspicious computer operations against a security policy, Matrix instead applies signatures to a "tokenized version of a Visual Basic Script, JavaScript, or HTML file to determine if there is a match." (*Id.*

(citing Tr. 1914:17-1915:3 ("Matrix is a signature scanner that looks for patterns in VBScript, JavaScript, and HTML content."); Tr. at 1920:2-15, 1920:25-1921:19, 1945:6-13).)

In addition, Symantec's expert, Dr. Bruce Maggs, also addressed each piece of evidence that Finjan relied upon to show infringement and explained why it did not support a finding of infringement. (*Id.* (citing Tr. at 1968:2-24, 1970:1-1974:10, 1976:1-1977:11 (Maggs)).) As further support, Symantec also directly rebutted, or at the very least cast doubt on, Finjan infringement expert, Dr. Medvoidovic's attempt to demonstrate the operation of the accused Matrix technology, by presenting evidence that his demonstration actually used a non-accused signature scanning component called the Trojan Scanner. (*Id.* (citing Tr. at 959:15-965:14, 967:9-974:13, 1923:8-1926:20, 1936:23-1937:8, 1961:7-1962:21).)

Moreover, in response to Finjan's assertion that Dr. Maggs conceded infringement because he acknowledged that a "signature" could include a list of suspicious operations, Symantec notes that its expert actually testified that the entire step of comparing the list of suspicious computer operations against a security policy is not performed. (*Id.* (citing Tr. at 1953:6-24 (Maggs) ("As I said, the whole claim element, starting with comparing by the server, is not met. . ."); Tr. at 1964:8-14, 1974:11-1975:25 (Maggs)).) To this end, Symantec disagrees with Finjan that the only disputed limitation of the '194 Patent at trial was "a list of suspicious computer operations." (*Id.* (citing D.I. 791 at 16).) Notably, Symantec argued that, even assuming that a signature includes a list of suspicious computer operations, that list would still need to be compared against a security policy to meet the claims—and Matrix does not do this. (*Id.*) Dr. Maggs testified to this point:

> Instead, in Matrix, you take these signatures that have been predefined by Symantec employees. One by one, you apply each signature to a tokenized version of the program. And you look for a match. And then you just record, was

> there a match or not. The way you do that is you record what was the identification number, the threat ID, of the signature.

(*Id.* (citing Tr. at 1955:20-1956:1; *see also* Tr. at 1971:19-1972:3 (Maggs)).) Ken Coleman, a Symantec engineer who wrote the code for Matrix, likewise testified and confirmed this testimony. (*Id.* (citing Tr. at 1915:1-1923:7; DX-4170).) Symantec asserts that, as Dr. Maggs and Mr. Coleman explained, the signature is applied to the tokenized file or "program" to determine if there is a match—nowhere is the signature compared against a security policy. (*Id.* (citing Tr. at 1944:12-1946:2).) Thus, Symantec argues that the evidence it presented demonstrates that "it is irrelevant whether the signatures include a list of suspicious computer operations, because the signatures are never compared against a security policy, as the claims require.[17] (*Id.* (citing Tr. at 1920:2-11).) In light of this evidence, Symantec argues that a reasonable jury could conclude that Matrix does not perform this claimed comparison.

Finally, Symantec's noninfringement evidence extended to challenging Finjan's assertion that its argument that the threat ID does not correspond to a list of suspicious computer instructions "was critically flawed because the asserted claims do not preclude the invention from labeling a list of suspicious operations with some type of identifier." (*Id.* (citing D.I. 791 at

[17] Symantec further notes that Finjan did not present any evidence or testimony that the Matrix signatures are compared to a security policy. Rather, Finjan's expert, Dr. Medvidovic, testified that the signatures or "script definitions" are used "to pluck out a set of tokens that turn out to be potentially malicious" and that "[t]hose tokens are the potential threats." (D.I. 810 at 16 (citing Tr. at 867:19-25, 871:1-9).) Dr. Medvidovic further testified that the list of suspicious computer operations correspond to a "tokenized downloadable" created after the signatures or "script definitions" are applied and did not argue that the signatures correspond to the list of suspicious computer instructions or that they are ever compared against a security policy. (*Id.* (citing Tr. at 868:19-25, 871:1-9).) Symantec disputed Dr. Medvidovic's characterization of Matrix at trial through the testimony of Mr. Coleman, who explained that no list of suspicious computer operations is ever extracted—or "plucked out"—from the tokenized file. (*Id.* (citing Tr. at 1919:1-1920:1, 1011:12-19, 1964:15-19).) Similarly, Dr. Maggs confirmed this point in testifying that "[t]here is never a step where you take, let's say, the tokenized representative of the JavaScript or Visual Basic Script and go out and pick out certain operations and put them on a list." (*Id.*) Dr. Medvidovic also confirmed this point on cross-examination, noting that "tokenization" "retain[s] all of the critical information from the code that you tokenized." (*Id.* (citing Tr. at 1011:12-19).) Thus, Symantec's expert and fact witnesses maintained that the tokenized file includes all operations, not merely the suspicious ones, which, Symantec contends, is sufficient evidence for the jury to conclude that the tokenized files do not correspond to the claimed list of suspicious computer operations. (*Id.*)

17).) Symantec argues that Finjan "misses the point" and that there is no list of suspicious computer operations. Instead, the "threat ID is just a number" that "does not contain a list of anything." (*Id.* at 16-17 (citing Tr. at 1921:7-11, 1956:2-18, 1965:22-1966:5).) If a match is identified after applying the signatures to the tokenized file, then a single threat ID—a number—is returned to the AV Engine by Matrix.[18] (*Id.* at 17 (citing Tr. at 1921:12-24, 1956:7-12).)

In consideration of the evidence presented at trial and the required JMOL standard, the court denies Finjan's motion with respect to the '194 Patent. Here, both Finjan and Symantec offered expert testimony explaining Symantec's Matrix product and whether it infringes the asserted claims of the '194 Patent. It is the province of the jury to assess the testimony of each expert witness and determine, viewed in light of the other evidence presented at trial, which was most credible and/or persuasive. Neither side presented evidence that went unchallenged and,

[18] Symantec also challenges Finjan's assertion that Symantec incorrectly argued at trial that Matrix does not generate Downloadable security profile data including a list of suspicious computer operations from the Downloadable code. (D.I. 808 at 17 (citing D.I. 791 at 17).) Symantec argues that, although the independent claims may not require "extracting" a list of suspicious computer operations from the Downloadable, all of the asserted claims "nonetheless require a list of suspicious computer operations." (*Id.*) Symantec further maintains that, according to the '194 Patent, "this list is obtained from the downloadable itself by disassembling the downloadable, resolving the commands, and determining whether each command is suspicious." (*Id.* (citing Tr. at 1953:25-1955:11; SYMDX12-9).) In contrast, Symantec and its expert contend that the signatures used by Matrix are created by Symantec employees and not derived from the Downloadable itself, supporting a noninfringement verdict. (*Id.* (citing Tr. at 1915:23-1916:15, 1955:20-21).)

Finjan is correct that the court did not construe "Downloadable security profile data pertaining to the Downloadable" to require, as the defendants argued, "data that was decomposed from the code for the receiving Downloadable." (D.I. 326 at 2 n.2.) Instead, the court construed the term as having its plain and ordinary meaning and noted, in rejecting the defendants' proposed construction, that the independent claim does not specify how the Downloadable security profile is generated, and instead simply requires "comparison." (*Id.*) Symantec's experts presented their interpretation of this claims based on the court's plain and ordinary meaning construction. *See LG Elecs. U.S.A., Inc. v. Whirlpool Corp.*, 798 F. Supp. 2d 541, 554 (D. Del. 2011) (noting that, where the court construes a disputed term to have its plain and ordinary meaning, the jury may consider any evidence at trial, including expert testimony, to understand the meaning of that term). The court acknowledges that its construction of this term did perhaps lend to some confusion, in that it construed the term to have a plain and ordinary meaning, but also noted in this construction that only "comparison," not "decomposing," was required by the claim.

As noted above, however, Symantec asserted and provided evidence to show that its Matrix product does not infringe this claim because it does not include a list of anything and Dr. Maggs testified that he confirmed this from the source code. (D.I. 810 at 17 (citing Tr. at 1921:7-11, 1956:2-18, 1965:22-1966:5).) Thus, regardless of Symantec's interpretation of this claim as requiring "decomposing," the evidence it provided was sufficient to demonstrate that Matrix did not include a list and could not meet the claim limitation. The court, therefore, concludes that any confusion resulting from the court's claim construction was not dispositive in assessing noninfringement. Symantec presented substantial evidence from which the jury could conclude that the Matrix product did not include a list and could not infringe this claim.

therefore, the jury was free to accept or reject the testimony of each witness in whole or in part. Thus, the court concludes that the evidence presented was sufficient for the jury's verdict of noninfringement.

b. Noninfringement of the '962 Patent

Finjan likewise maintains that the court should grant its motion for JMOL as to Symantec's noninfringement of the asserted claims of the '962 Patent. (D.I. 790; D.I. 791.) Specifically, Finjan argues that a reasonable jury could only find that Symantec infringes the '962 Patent because it performs each of the three claim limitations that Symantec disputed at trial: (1) "performing a predetermined responsive action based on the comparison"; (2) "interrupting the processing of the request"; and (3) "operating system interfaces." With respect to the first limitation, Finjan contends that it was undisputed at trial that BASH performs a predetermined action of allowing "good" files to execute, thus meeting this limitation. (D.I. 791 at 18.) In addition, Finjan notes that, with regard to "bad" or malicious Downloadables, "Finjan's expert presented substantial, irrefutable evidence of infringement at trial," through, for instance, pointing to source code demonstrating that the "reputation" or "exoneration check" is part of the "security policy."[19] (*Id.* at 18-19 (citing Tr. 784:6-25, 810:12-811:11).) Thus, Finjan argues, Symantec's contention that BASH does not infringe because it does not always perform "a predetermined responsive action" is unsupported.

Regarding the second limitation, Finjan asserts that it proved by substantial evidence that Symantec infringes this limitation because it is Symantec—not Microsoft—that performs the step of this limitation. (*Id.*) Specifically, Finjan asserts that it demonstrated that Symantec's

[19] Finjan also notes that its infringement case is supported by: (1) Symantec's technical documents, which listed predetermined responsive actions taken after a security policy "check" or "comparison" (D.I. 791 at 19 (citing Tr. at 1997:15-16 (Dr. Maggs point to "possible types of responses that could be taken" after the "reputation check"); and (2) the testimony of Mr. Satish, Symantec's co-developer of BASH, who testified that the "reputation check" is not always performed and if the Downloadable was bad, it may be immediately remediated" (*id.* (citing Tr. at 1045:15-1047:15))).

BASH was, in fact, "interrupting" and notes that it showed the BASH architectural design to the jury and that this design makes clear that it is the Symantec drivers that carry out the "interrupting" process. (*Id.* (citing Tr. at 748:6-753:9, 802:10-803:8, 805:2-809:25, 819:14-820:16, 828:12-829:9, 833:18-834:11, 834:19-835:25, 843:11-844:15).) Finjan also details that Dr. Medvidovic's testimony, the BASH technical guide, and an Integration Functional Specification, all presented at trial, support its contention that it is Symantec that performs the "interrupting" function. (*Id.* (citing Tr. at 741:4-742:13, 748:6-749:9, 827:6-828:2, 835:4-19; Ex. 14, PTX-868).) Similarly, with respect to the "operating system interfaces" limitation, Finjan argues that Symantec failed to rebut the substantial evidence it presented that BASH has the "operating system interfaces" detailed in Claims 12 and 15 and that this operating system is not provided by Microsoft.[20] (*Id.* at 20.) Finjan states that it demonstrated this fact by introducing Symantec technical documents and source code showing that BASH meets this limitation. (*Id.* (citing Ex. 1, Tr. at 728:12-739:17, 775:2-777:25).)

For reasons similar to those stated above in connection with examination of Symantec's noninfringement position regarding the '194 Patent, the court finds that Symantec presented evidence sufficient for a reasonable jury to find that its BASH product does not infringe the '962 Patent. Specifically, it is clear to the court that, contrary to Finjan's assertion that the evidence it presented was irrefutable, both sides presented evidence, supported by expert testimony, which the jury was free to assess. For instance, Symantec contends that it did, in fact, present a noninfringement argument that consisted of evidence that, if the jury deemed credible, demonstrates that Symantec's accused product does not: (1) perform "a predetermined

[20] Finjan argues that Symantec's expert, Dr. Maggs, had no rebuttal for the evidence presented and, instead, simply stated "in a conclusory fashion" that "[t]hese aren't operating system interfaces," without providing any "substantive explanation." (*Id.* at 20 (citing Tr. at 1989:19-1990:15).)

responsive action based on the comparison"; (2) perform the "interrupting processing of the request" limitation; and (3) provide the "operating system interfaces." (D.I. 810 at 17-20.)

In support of its first contention, Symantec argues that the "evidence showed that the accused BASH technology does not perform 'a predetermined responsive action based on the comparison,' as required by the asserted claims because BASH performs a reputation check before taking any action." (*Id.* at 17 (citing Tr. at 1981:9-12, 1989:16-1994:5).) The reputation is not "predetermined," because it can change at any moment. (*Id.* (citing Tr. at 1993:13-1994:5).) Symantec also asserts that, contrary to Finjan's argument that Symantec did not dispute that no "reputation check" is performed in the case of "good" Downloadables, it was Finjan that failed to prove this point. (*Id.* at 18.) Specifically, Symantec notes that the only evidence Finjan cites in support of this argument is the deposition testimony of Symantec engineer, Mr. Satish, which was played during trial. In particular, Mr. Satish responded "correct," to the question "[a]nd then if the disposition returned by BPE is good, then the activity is allowed to go through. Correct?" (*Id.* (citing Tr. at 1047:12-15).) Symantec argues that this testimony is insufficient to establish that there is no reputation check in the case of "good" Downloadables because, for example, it would be entirely consistent with Mr. Satish's testimony that the reputation check could occur before the BPE returns "good." (*Id.* (citing Tr. at 1993:20-22 ("After BASH comes up with a tentative action, there is always this last step of going out to the reputation system."), 1843:10-1844:1).) Notably, Finjan's expert did not testify as to the alleged infringement by good Downloadables. (*Id.*)

Moreover, Symantec argues that Finjan's infringement contention with respect to "bad" Downloadables was not supported by substantial, irrefutable evidence. (*Id.*) To the contrary, Symantec notes that Mr. Nachenberg, the inventor of Symantec's reputation technology, testified that "BASH will not block a file even if its behavior is suspicious unless that file also has a certain threshold, low level of reputation, where it will say it is also not associated with sterling users, for instance." (*Id.* at 18-19 (citing Tr. at 1843:10-16).) In addition, Dr. Maggs explained that reputation is not predetermined "because the reputation of a file can change day by day, hour by hour, even minute by minute." (*Id.* at 19 (citing Tr. at 1993:13-1994:5).) Dr. Maggs supported his testimony by showing the BASH source code where the reputation check occurs and by addressing each document Finjan presented in support of its theory, explaining why that evidence was insufficient to prove infringement. (*Id.* (citing Tr. at 1994:22-1995:24, 1995:25-2002:10; PTX-868-14).)

Further, and with regard to the second limitation asserted in the '962 Patent, Symantec notes that Finjan cites extensively to the testimony of its expert, Dr. Medvidovic, but ignores the contrary testimony of Dr. Maggs, who presented evidence that the claimed "interrupting" is performed by Microsoft and, further, that the operating systems of BASH are likewise Microsoft provided. (*Id.* at 19-20 (citing Tr. at 1981:3-8, 1987:25-1988:6).) For the "interrupting" claim, Dr. Maggs relied upon Microsoft's website to show that the filter manager provided by Windows "actually does the interrupting" when requested, as well as on Symantec's source code and confidential documents to support his position. (*Id.* at 19 (citing Tr. at 1981:18-1982:6, 1982:25-1985:4; SYMDX-12-4; DX-4322).) For instance, Dr. Maggs explained that, per Symantec's technical document, BASH would not work without the filter manager Windows provided. (*Id.* (citing Tr. at 1983:8-1986:13; PTX-1083-7).) Again, Dr. Maggs reviewed each piece of evidence Dr. Medvidovic provided and explained why it did not show that the BASH product infringes. In fact, Symantec references Dr. Medvidovic's testimony on cross-examination that, among other things, the set of filters "exists within an operating system," and that Symantec's probes are "implement[ed] on top of Windows." (*Id.* at 20 (citing Tr. at 997:1-1001:18, 1000:17024, 1982:7-24, 2030:6-2031:14).) Dr. Medvidovic also did not rely on source code for his infringement analysis of this limitation. (*Id.* at 19 n.8 (citing Tr. at 1996:2-5).)

Similarly, Symantec correctly notes that Finjan focuses its JMOL motion with respect to the third limitation on Dr. Medvidovic's testimony, while avoiding Dr. Maggs testimony. Indeed, Dr. Maggs testified that "Microsoft provides the operating system interfaces" and further explained that Microsoft seeks to provide these interfaces in order to "control . . . the stability of the operating system." (*Id.* at 20 (citing Tr. at 1987:25-1988:6, 1988:7-1989:14).) Dr. Maggs also explained that the "interfaces" described in Symantec's documentation refers to other parts of the code—not the operating system interfaces—and that nothing in PTX-1076-19 describes such interfaces. (*Id.* (citing Tr. at 1989:19-1990:15; PTX-1076-19).)

In view of the foregoing and for the reasons stated in connection with denial of Finjan's '194 Patent JMOL motion, the court finds that both sides presented evidence of noninfringement through exhibits, fact, and expert testimony, such that the jury had reasonable grounds to find noninfringement on substantial evidence. The court will not, therefore, overturn the jury's verdict or assessment of the evidence presented to it.

3. The Jury's Finding of Websense's Noninfringement

Finjan asserts that a reasonable jury could only find that Websense infringed the asserted claims of the '194 Patent because: (1) Websense's RTSS technology uses a "list of suspicious computer operations" (D.I. 788 at 3-6); (2) Websense's RTSS compares downloadable security profile data using a "server that serves as a gateway" (*id.* at 6-7); (3) Websense's RTSS decomposes Downloadables into DSP data (*id.* at 7-8); and (4) there was overwhelming evidence at trial that Websense willfully infringed the '194 Patent (*id.* at 8-10).

First, and in support of its infringement position regarding the "list of suspicious computer operations" claim, Finjan maintains that Websense's principal noninfringement argument that its accused RTSS technology does not use a "list of suspicious computer operations" is entirely unsupported by the evidence. Specifically, Finjan contends that this argument fails because it is premised on reading two non-existent limitations into the claims—specifically, that: "(1) the list of suspicious operations is *generated* in real time (as opposed to *used* in real time, as the claims require); and (2) the suspicious operations cannot be detected by matching text (even though the claims require only "comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list of suspicious computer operations that may be attempted by the Downloadable")." (D.I. 788 at 4.)

With regard to the former, Finjan notes that Websense's noninfringement argument at trial was that the claimed "list of suspicious computer operations" must be generated from the Downloadable code in real-time, and that this limitation is not satisfied when RTSS uses information created "offline" in Websense's "ThreatSeeker Labs" to search for malware." (*Id.* (citing Tr. at 2796:19-20, 2799:12-21, 2858:18-2859:1).) Finjan maintains that this argument is inconsistent with the court's claim construction of this term, which specifically rejected the defendants' argument that the limitation requires that the security data be generated from the Downloadable itself. (*Id.* (citing D.I. 326 at 2 n.2).) Thus, Finjan argues that Websense's noninfringement position was contrary to the law of the case. (*Id.*) Moreover, Finjan asserts that because RTSS "undisputedly searches in real-time for threats by using a list of data that pertain to Downloadables," this limitation is clearly met. Regarding the latter argument, Finjan asserts that Websense's improperly argued at trial that RTSS does not use a list of suspicious operations because it only examines Downloadables by searching for matches of plain "text" signatures. (*Id.* at 5.) Because, Finjan contends, the asserted claims do not specify how the list of suspicious operations is used to inspect Downloadables, it does not exclude searching for text corresponding to suspicious operations. (*Id.* (citing Ex. 3, '194 Patent at 10:11-15 (Claim 1)).)

Second, Finjan asserts that Websense's noninfringement defense that RTSS does not have the claimed "server that serves as a gateway" because it uses two different servers to perform the claimed comparison—one at the gateway and one not at the gateway—was entirely unsupported at trial and based on an incorrect claim construction position. Specifically, Finjan argues that Websense's documents and witnesses proved that the alleged second "policy server' was functionally part of the same server "that serves as a gateway" and, therefore, is covered by the asserted claims. (*Id.* at 6 (citing Tr. at 1320:1-21, 1343:11-23, 1367:1-1369:7, 1376:10-22).) Third, and with regard to the "decomposing the Downloadable into Downloadable security profile data" limitation, Finjan contends that the jury's verdict of noninfringement went against the weight of the evidence because it "presented substantial evidence that RTSS performs this step by parsing Downloadables (i.e., breaking the HTML down into elements)" and Websense's expert "effectively conceded" this point in testifying that: "[t]he parsing that is taking place here is breaking HTML content into various types of buffers that will be scanned by specific groups of signatures."[21] (*Id.* at 8 (citing Tr. at 2886:23-25; JTX-406 at WEBS 01026172).) Finally, Finjan maintains that it was clear from the substantial evidence presented at trial that Websense's infringement was willful based on its monitoring of Finjan as a competitor, knowledge of Finjan's patents, and specific knowledge of the '194 Patent. (*Id.* at 8-13.)

[21] In support, Finjan also cites to Websense's expert, Ms. Frederiksen-Cross' testimony that the "bloom filter" component, at the very least, is "part of the process used to see if a particular piece of the [D]ownloadable may go on to be matched by threat profiles." (D.I. 788 at 8 (citing Tr. at 2965:9-11).) Finjan asserts that this testimony acknowledges that RTSS decomposes Downloadables into pieces to be analyzed. (*Id.*)

Conversely, Websense argues that the jury finding was, in fact, reasonable and supported by substantial evidence because: (1) every disputed term of the '194 Patent, except "Downloadable," was construed to have its plain and ordinary meaning, such that the parties were allowed to provide expert testimony as to a person of ordinary skill in the art's understanding of those terms; (2) Websense's expert, Ms. Frederiksen-Cross, who Finjan stipulated was of ordinary skill in the art, explained the disputed terms to the jury as she understood them; (3) Finjan's own experts agreed with Ms. Frederiksen-Cross' understanding of these terms; and (4) the accused RTSS module does not use any list of suspicious computer operations, as required by the "list of suspicious computer operations" claim. (D.I. 808 at 7-15.) Websense also maintains that the jury's finding of no willful infringement is likewise supported by substantial evidence. The court agrees that the jury verdict of noninfringement is supported by substantial evidence and will address each argument in turn.[22]

[22] Websense argues, as an outset consideration, that Finjan has waived its Rule 50(b) JMOL arguments because it failed to assert the grounds in its Rule 50(a) motion. (D.I. 808 at 4.) Websense maintains that Finjan did not, as is required, raise the grounds for its Rule 50(b) motion in its Rule 50(a) motions—namely, Websense's introduction of a person of ordinary skill in the art testifying to their understanding of the plain and ordinary meaning of the terms in the '194 Patent. (*Id.*) Specifically, Websense argues that Finjan did not raise this issue in connection with: (1) the term Downloadable security profile data must be generated at the gateway; and (2) whether the parsing of Downloadables by its RTSS module satisfied the decomposing limitation in Claim 2. (*Id.* (citing D.I. 733 at 5-6; Tr. at 2983:7-11).) Websense asserts that Finjan's failure to provide adequate notice of these new arguments deprived Websense of the chance to cure any evidentiary defects during trial and should, therefore, be deemed waived. (*Id.* (citing Rule 50, Advisory Committee Notes to 1991 Amendment ("The purpose of the requirement is to assure the responding party an opportunity to cure any deficiency in that party's proof that may have been overlooked until called to the party's attention by a late motion for judgment.").

The court disagrees and finds that Finjan did, in fact, preserve its infringement arguments by asserting them in its Rule 50(a) motion and by citing to infringement evidence in the record. (D.I. 821 at 7-8.) Specifically, in its Rule 50(a) motion, Finjan identified what it viewed as substantial evidence at trial and cited to the record to demonstrate that Websense failed to rebut this evidence. (*See* D.I. 733.) The Federal Circuit has made clear that even a cursory motion suffices to preserve an issue on JMOL so long as it "serves the purpose of Rule 50(a), i.e., to alert the court to the party's legal position and to put the opposing party on notice of the moving party's position as to the insufficiency of the evidence." *See, e.g., Western Union Co. v. MoneyGram Payment Sys., Inc.*, 626 F.3d 1361, 1367 (Fed. Cir. 2010) (citation omitted); *Tex. Instruments Inc. v. Cypress Semiconductor Corp.*, 90 F.3d 1558, 1566 n.6 (Fed. Cir. 1996) (finding pre-verdict motion requesting judgment of no infringement sufficient to support post-verdict motion concerning the doctrine of equivalents); *Malta v. Schulmerich Carillons, Inc.*, 952 F.2d 1320, 1324-25 (Fed. Cir. 1991) (same).

In addition, the court also finds that Finjan did not waive its right to dispute Websense's expert's interpretation of the "plain and ordinary meaning" of the term "Downloadable security profile data includes a list of suspicious computer operations." Contrary to Websense's assertion that Finjan failed to object to this testimony at

First, and with regard to Ms. Frederiksen-Cross' testimony as to her understanding of "what . . . downloadable security profile data is," Websense argues that, because the disputed term was given its plain and ordinary meaning, her understanding of the claim term was relevant evidence for the jury to consider and was not improper claim construction. (*Id.* at 7 (citing *LG Elecs. U.S.A., Inc.*, 798 F. Supp. 2d at 554; *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1326 (Fed. Cir. 2012) ("It was up to the jury to determine from the evidence presented at trial whether the ActiveVideo system satisfied the plain and ordinary meaning of the 'superimposing' limitations.")).) Websense notes the relevancy of her interpretation is reinforced by the Jury Instructions in this case, which tasked the jury with determining the meaning of those terms for which they were not provided a definition. (*Id.* (citing Tr. at 3236:15-3237:5).) Ms. Frederiksen-Cross explained her understanding of the terms in the '194 Patent during trial:

> Q: What is your understanding of what the downloadable security profile data is?
> A: The downloadable security profile is information that pertains to the specific downloadable in the specification. And you heard Dr. Medvidovic say that, you know, it's extracted from the downloadable. So it's information that comes right out of that downloadable, and that includes this list of suspicious operations.

(*Id.* (citing Tr. at 2867:13-20).)

Websense also asserts that Finjan experts, Drs. Medvidovic and Vigna, both agreed with this interpretation. Specifically, Websense cites to Dr. Vigna's statement that the '194 Patent requires extraction of Downloadable security profile data that includes a list of suspicious

trial, Finjan's counsel objected to this testimony in advance of Ms. Frederiksen-Cross' direct examination. (D.I. 821 at 8 (citing Tr. at 2837:1-2841:8).) Specifically, Finjan's counsel objected to this expert witness "using the prosecution history to sneak in a new claim construction that was contrary to the [c]ourt's claim construction:

> I just don't want this jury to be prejudiced—this kind of blends into the second argument. I just don't want this jury to be focusing on the file history for infringement purposes and trying to take the [c]ourt's claim construction, which is plain and ordinary meaning, and try to read limitations from the prosecution history, the specification, or for that matter, into it.

Tr. at 2840:18-24. While the court allowed Ms. Frederiksen-Cross to provide this testimony at trial, the court concludes that it is clear that Finjan noted its objection to this testimony on the record.

computer operations at the gateway,[23] as well as to Dr. Medvidovic's testimony agreeing that the patent requires that a list of suspicious computer operations be presented online and extracted online at the gateway.[24] (*Id.* at 8.) Thus, Websense argues that "Finjan cannot be heard to complain now that Websense's expert understood the term 'pertaining to the Downloadable' to mean that the DSP data must be extracted at the gateway, because that testimony comes originally from Finjan's own experts." (D.I. 808 at 9.) Websense also notes that Finjan had used the extraction of the list of suspicious computer operations at the gateway, as opposed to signatures created beforehand by off-line human researchers, as a point of novelty for the '194 Patent. (*Id.* at 9 (citing Batcher Decl., DJX0410 at 12-13; *see also* Tr. at 436:23-438:14, 476:14-477:19, 1498:6-15).)

Notably, Finjan clarifies, however, that its experts did not understand "extract" to have the same meaning as Websense's expert. In particular, Finjan details that Drs. Medvidovic and Vigna did not understand "extract" to mean "generate" and testified to that effect, stating that "extract" is synonymous with "identify." (D.I. 821 at 4 (citing Tr. at 496:2-19, 1441:9-14, 1479:7-12).) It appears to the court that Finjan is correct in noting that Drs. Medvidovic and Vigna did not use "extract" in the same way as Websense's expert and, therefore, did not reach the same conclusion as to the meaning of the disputed term.

[23] Websense cites to Dr. Vigna's testimony that: "[t]he '194 Patent focuses on the gateway, so the basic idea is the patent that describes the technology that operates at the gateway and receives this new threat, extracts what operation they might possibly execute, and by comparing me [sic] with a security report is to decide if this security is to be let go or to be—let go to the client or to be blocked." Tr. at 441:5-14; *see also id.* at 475:3-9 ("Yes, I think that the concept of the '194 Patent was to extract a profile from this downloadable that contains a list of operations.").

[24] Dr. Medvidovic testified:

> Q: This word operations becomes fairly important to this Claim 1 of the '194 Patent. Right? Because this Patent requires that a list of suspicious computer operations be present online, extracted online at the gateway. Right?
> A: Yes.
> Q: And so in order to infringe there has to be list of suspicious operations, as you said, that gets extracted at the gateway?
> A: I might have said that, sure.

Id. at 1497:9-17; *see also id.* at 1440:20-23.

Websense further argues, regardless of the conflicting interpretation of "extract" and Ms. Frederiksen-Cross' interpretation of the plain and ordinary meaning as requiring "extracting" or "decomposing," its RTSS analytic "does not use a list of suspicious computer operations at all, let alone one generated or extracted at the gateway." (D.I. 808 at 9.) In fact, Ms. Frederiksen-Cross testified that Websense's accused analytic does not "contain the logic that is capable of identifying or determining that a particular string of text is in [sic] operation" and "does not have the ability to evaluate any aspect of the behavior." (*Id.* (citing Tr. at 2861:13-18).) Instead, Websense's analytic "merely signature matches" and uses "a more traditional signature-scanning approach." (*Id.* (citing Tr. at 2876:25-2877:9, 2881:12-2883:20 ("I have studied some of these threat profiles and it's very clear that they are not just lists of suspicious operations.")).) Websense notes that it also presented documents and fact witnesses confirming that its RTSS analytic only uses signature-based pattern-matching, and not a list of suspicious operations. (*Id.* (citing Tr. at 2663:23-2664:7, 2794:7-8, 2801:7-2803:9; Batcher Decl.; Ex. D [JTX-406]; Ex. E [JTX-417]).) Thus, Websense asserts that it presented substantial evidence that, if accepted by the jury, would result in a reasonable verdict of noninfringement in connection with the "list of suspicious computer operations" limitation.

The court agrees. As explained in connection with Finjan's similar argument with respect to Symantec's Matrix technology, the court's claim construction of this term may have generated some confusion, in that the term was construed to have a plain and ordinary meaning, but the court's construction also rejected the defendants' *Markman* argument that "decomposing" is required by the claim language. However, as the court found regarding Symantec, here, Websense presented substantial evidence from which the jury could conclude that the Websense technology did not include a "list" and, therefore, did not meet the claim limitation.[25]

Second, Websense contends that it presented sufficient evidence for the jury to find that RTSS does not infringe the "using a server that serves as a gateway to the client and compares the Downloadable security profile data against a security policy" limitation. Specifically, Websense maintains that substantial evidence supports the jury's conclusion that Websense's policy server does not serve as a gateway to the client, such as: (1) JTX-423, which shows both a "gateway server" or "WTG" and a separate "policy server [which] is a part of the legacy Web Filter server" (*Id.* at 10 (citing Tr. at 2922:13-16; JTX-423 at WEBS 01082644)); (2) JTX-441, showing that Websense customers even had to install the Websense policy server separately from installing the Websense proxy server (WCG) (*id.* (citing JTX-441 at WEBS 00093240; Tr. at 2923:13-2924:18)); (3) JTX-365, demonstrating that Websense customers can separately license the product that contains the Websense policy server from the product containing the gateway proxy server (*id.* (citing JTX-365 at WEBS 00134197; Tr. at 2925:10-2926:1)); and (4) Websense's source code, showing that the policy server is separate from the gateway proxy server (*id.* (citing Tr. at 2926:4-12)). In light of this evidence, Ms. Frederiksen-Cross testified that Websense's policy server only compares Websense's "category" and "reason" codes returned by the RTSS to a security policy, but does not receive a Downloadable addressed to a client and does not serve as a gateway to the client. (*Id.* (citing Tr. at 2922:9-2926:12).)

Further supporting this conclusion, Websense asserts that Finjan "relies upon misstatements and mischaracterizations of the document evidence and witness testimony," for instance citing to the deposition of Websense engineer, Hai Nguyen, to suggest that Websense's policy server acts as a gateway, when he was testifying about the proxy, not policy, server. (*Id.*

[25] *See supra* note 18.

at 11 (citing Tr. at 1320:9-21).) Moreover, Websense maintains that, contrary to Finjan's assertion in its Opening Brief in Support of JMOL, Ms. Frederiksen-Cross did not state that the policy server and proxy server functioned together as a gateway, but instead testified that the policy server is distinct from the gateway server and only performed a comparison to the security policy, not to a list of suspicious computer operations. (*Id.* (citing Tr. at 2922:9-2923:12, 2973:12-2974:7).) Finally, Websense clarifies that Ms. Frederiksen-Cross testified that the physical presence of two servers within a single "box" did not make those two servers a single server that serves as a gateway. (*Id.* (citing Tr. at 2972:25-2974:7).)

In view of the foregoing, the court concludes that the jury's finding of noninfringement with respect to this claim limitation is supported by substantial evidence. Indeed, the court agrees with Websense that Finjan's arguments for infringement center on issues of conflicting evidence and expert testimony regarding Websense's policy server and, therefore, are insufficient to set aside the jury verdict.[26] *See Energy Transp. Group, Inc. v. Sonic Innovations,*

[26] The court notes that Finjan also argues that Websense infringes by using a "server that serves as a gateway" to "compar[e]" the Downloadable security profile data" against a security policy and that this finding is supported by the substantial evidence Finjan introduced showing that Websense infringes under the stipulated definition of "a server" as "one or more servers." (D.I. 821 at 5.) Specifically, Finjan asserts that the asserted patent claims do not require that the "server" be a single, physical server, such that Websense's noninfringement argument that it has a "policy server" that is physically separate, can be installed by itself, and, therefore, is not the claimed "gateway server," is incorrect. (*Id.*) In addition to quoting the language from Claim 1, which reads "[a] computer-based model, comprising the steps of: receiving an incoming Downloadable addressed to a client, by a *server that serves as a gateway to the client*, comparing, *by the server*," Finjan also cites in support, its expert's testimony providing the same interpretation, as well as Ms. Frederiksen-Cross' testimony that "from the very beginning, where a request comes in," there is a "back and forth between the two servers" where they communicate via a "WISP communication that's document." (*Id.* (citing '194 Patent, Claim 1 at col. 10, ll. 8-18; Tr. at 2926:6-10; Tr. at 1342:25-1343:6).) Finjan further maintains that Mr. Nguyen's description of the accused product as a "proxy" only supports a finding of infringement because he describes a "proxy" that "sits in between the users and the Internet," which, Finjan argues, is a "gateway." (*Id.* at 6-7 (citing Tr. at 1320:1-21).) Finjan argues that, because the "policy server" performs "a comparison to the security policy," as Websense acknowledged in its Brief in Opposition, the jury could not have reasonably found that the accused product does not infringe. (*Id.* at 7 (citing D.I. 808 at 11).)

In view of the evidence before, the court finds that the jury's noninfringement verdict is based on substantial evidence and, thus, rejects Finjan's request to set it aside or order a new trial. Websense argued at trial that Claim 1 of the '194 Patent requires that the "comparing" be done by "the server," which is "a server that serves as a gateway to the client," and does not allow a non-gateway server to perform the Downloadable security profile data comparison, as Finjan asserts. (D.I. 808 at 12.) To this end, Websense cites to the same language Finjan quotes in Claim 1, but argues that the term "the server" in line 11 is the same "server" as in line 10 of Claim 1," because "a server that serves as a gateway to the client" is the antecedent for "the server" in line 11. (*Id.* at 12-13 (quoting *e.g.*, *Inc.*, C.A. No. 05-422 (GMS), 2011 WL 2222066, at *21 (D. Del. June 7, 2011) ("[T]he court will not disturb the jury's credibility determinations or substitute resolution of the conflicting evidence for that of the jury.").

Third, Websense maintains that Finjan's JMOL motion should be denied with respect to the "decomposing the Downloadable into Downloadable security profile data" recited in Claims 2 and 66, because the jury finding of noninfringement was based on substantial evidence. Contrary to Finjan's contention that it demonstrated that RTSS performs this step by "parsing Downloadables (i.e., breaking the HTML down into elements)," Websense argues that its RTSS product does not meet this limitation because it "parses HTML content into various buffers for signature scanning," but "cannot and does not identify operations." (D.I. 808 at 14 (citing Tr. at 2886:16-2887:23, 2861:5-18; JTX-406 at WEBS 01026169-73; JTX-417).) Therefore, as Ms. Frederiksen-Cross testified, "none of the accused Websense products is capable of decomposing a Downloadable into Downloadable security profile data *that includes a list of suspicious computer operations*." (*Id.* (emphasis in original) (citing Tr. at 2801:7-2803:9).) Ms. Frederiksen-Cross also testified that the "Bloom Filter" has nothing to do with decomposing or parsing content into a list of suspicious operations and is instead a pre-screen to remove content that would not be matched by a subsequent signature, rejecting Finjan's assertion that Ms.

Zoltar Satelite Alarm Sys. v. Motorola, Inc., No. C 06-00044 JW, 2007 U.S. Dist. LEXIS 9552, at *29 (N.D. Cal. Dec. 21, 2007) ("Under the conventions of claim drafting . . . the first time a part is mentioned, it should be preceded by the indefinite article 'a,' i.e., 'a selection circuit.' Subsequent references to that circuit should be preceded by the definite article 'the' or with 'said.'")).) Websense cites to several Federal Circuit cases in support. *See id.* at 13. Websense also maintains that this interpretation comports with the prosecution history of the '194 Patent. In particular, Websense notes that, in order to overcome the prior art, the applicant amended Claims 1, 32, and 65 to include the limitation "a server that serves as a gateway to the client." (*Id.* at 13 n.6 (citing DJX-0135 at 177-85).) Thus, Websense contends that Finjan's argument that Claim 1 permits multiple servers because "a" means "one or more" servers is "beside the point," as "[e]ach such server must still 'serve as a gateway to the client.'" (*Id.*at 13-14.) Websense cites to the exchange between its counsel, Mr. Grimm, and Finjan's counsel, Mr. Hannah, as further support for its understanding of the parties stipulated agreement to the meaning of server. (*Id.* at 14 (citing Tr. at 2920:17-2921:6).) Considering the evidence presented at trial detailed above, the court concludes that Websense presented substantial evidence that its policy server does not serve as a gateway to the client, argued that the "one or more must be the same one or more" server, and, therefore, provided the jury with evidence sufficient for it to reasonably conclude that Websense did not infringe the '194 Patent.

Frederiksen-Cross conceded infringement of this step when she testified that the "bloom filter" is "part of the process used to see if a particular piece of a Downloadable may go on to be matched by threat profiles." (*Id.* at 14-15 (citing Tr. at 2886:16-2887:23).)

Finjan asserts that Ms. Frederiksen-Cross' testimony acknowledges that RTSS decomposes Downloadables into pieces to be analyzed," which would meet the limitation. (D.I. 788 at 8; D.I. 821 at 7.) Specifically, Finjan argues that, even if RTSS "does not contain the logic that is capable of identifying," as Websense asserts, it still infringes because: "all the claims require is that the Downloadable security profile data includes a 'list of suspicious operations'"; "'operations' are identified from the Downloadable elements, and the process of identification is not restricted by the claims"; and regardless of whether the "bloom filter" is a pre-screen, it still infringes because "a particular piece of the Downloadable may go on to be matched by threat profiles." (D.I. 821 at 7.)

In consideration of the record before it and the parties' arguments, the court disagrees with Finjan that the jury verdict was not based on substantial evidence. While Finjan is correct that Dr. Medvoidovic comprehensively explained why, in his opinion, RTSS infringes the "decomposing the Downloadable into Downloadable security profile data" limitation in Claims 2 and 66, Ms. Frederiksen-Cross likewise presented her opinion. In fact, in stating her opinion, Ms. Frederiksen-Cross directly challenged Dr. Medvoidovic's findings, expressing disagreement with his overall opinion and explaining that his analysis was, in her view, inaccurate due to incomplete understanding of the RTSS process. Ms. Frederiksen-Cross also explained to the jury why the RTSS system does not infringe the asserted claims and did so by detailing her understanding of each claim and the product. Thus, it is clear to the court that Websense presented a noninfringement defense and that the jury, if it agreed with Websense's expert, could find noninfringement based on substantial evidence.

Finally, Finjan requests that the court set aside the jury verdict with respect to the jury's willful infringement finding, because it provided substantial evidence that Websense knew of the '194 Patent before June 2008.[27] (D.I. 788 at 8-13.) Specifically, Finjan argues that Websense was aware of Finjan's patents, "plainly recognized the danger that Websense's products would infringe the '194 Patent, and, nevertheless, developed and sold the accused products despite an objectively high likelihood that its actions constituted infringement. Finjan maintains that this "objectively-defined risk was either known or so obvious that it should have been known to Websense," resulting in willful infringement. (*Id.* at 8 (citing *In re Seagate Tech., LLC*, 497 F.3d 1360, 1371 (Fed. Cir. 2007)).)

Finjan details that it presented, as a sampling of the evidence introduced at trial: (1) that Websense began monitoring Finjan, its patents, and its products, starting in 2005, as shown by an email to Dan Hubbard, Websense's Chief Technology Officer, describing research into Finjan's patents and sent in response to Hubbard's email forwarding an article regarding Microsoft's licensing of Finjan's security patents (*id.* at 9 (citing Tr. at 1309:1-1310:24, 1312:9-14, 2822:4-2823:15, PTX-1367)); (2) Mr. Hubbard's testimony that he was aware, at the time he sent the referenced email, that Finjan had patents (*id.* (citing Tr. at 1310:16-24)); (3) Websense did "competitive testing" of Finjan's products and frequently reviewed its website and white papers (*id.* (citing Tr. at 2819:8-9)); (4) Websense's Board of Directors had discussions about Finjan, cross-licensing, and other strategies to "get around patent issues," according to Mr. Hubbard's testimony (*id.* at 10 (citing Tr. at 2823:16-21)); (5) in October 2006, Websense was developing

[27] The court notes that Websense stipulated that it was aware of the '194 Patent as of June 6, 2008, the date that it filed a reexamination request of that Patent. (D.I. 808 at 15 n.7.)

its web security gateway product and at least five Websense participants, including Mr. Hubbard and other managers, scheduled a conference call to "Discuss Finjan History, capability, ip and partnering prospects" (*id.* (citing PTX-1331)); (6) there was a December 2007 email exchange in which Websense's CEO and President, among others discussed boards that Websense's CEO and former CEO should be on and, in that exchange, Mr. Hubbard recommended joining Finjan's board "mostly for patent protection and future IP" because he "believe[d] there is a strong chance they could come after us post Dorado[28] release" (*id.* at 11 (citing PTX-1397; Tr. at 1312:15-1313:25)); and (7) Shlomo Touboul, former Finjan CEO, testified that Finjan always marked its products, either with "patent pending" or with patent numbers after the patents were issued, such that Websense would have been aware of them[29] (*id.* at 12 (citing Tr. at 532:10-18).)

Conversely, Websense contends that Finjan has failed to demonstrate willful infringement by clear and convincing evidence because Finjan has not introduced evidence sufficient to show that Websense knew of the '194 Patent prior to June 6, 2008. (D.I. 808 at 15.) Moreover, Websense argues that, in light of the evidence in the record and the jury's finding that the '194 Patent is invalid, it is clear that there was no objectively-high likelihood of infringement as required for a willful infringement claim. (*Id.* (citing *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1336-37 (Fed. Cir. 2009) (affirming JMOL of no willfulness where the defendant presented a "substantial question" of noninfringement)); *Spine Solutions v. Medtronic Sofamor Danek USA*, 620 F.3d 1305, 1319-20 (Fed. Cir. 2010) (finding that the accused infringer raised a "substantial question" of obviousness sufficient to defeat a charge of

[28] The "Dorado release" refers to Websense's development of an accused web security gateway product. (D.I. 788 at 11 n.5.)

[29] Finjan also notes that, though the court did not allow the evidence at trial, it was prepared to introduce evidence that Websense monitored Finjan's lawsuit against Secure Computing in which the '194 Patent was asserted. (*Id.* at 12-13.) Finjan renews its request that this evidence be considered as proof of Websense's willful infringement. The court will not, however, consider this evidence in assessing whether the jury verdict was reasonable and based on substantial evidence because the jury did not hear it. *See Goodman v. Pa. Turnpike Comm'n*, 293 F.3d 655, 665 (3d Cir. 2002).

willfulness)).) In view of the relevant law, the evidence presented, and the jury's verdict, the court agrees with Websense that Finjan has not demonstrated that there was an objectively-high likelihood of infringement.

In addition, the court also finds that the jury could have reasonably concluded, based on the evidence Finjan presented, that Websense did not subjectively think it infringed the '194 Patent. For instance, Websense notes that Mr. Hubbard testified that the email from Joe Jarcoch addressed to him, which Finjan cites as PTX-1367, did not identify the '194 Patent. (D.I. 808 at 16 (citing PTX-1367).) In addition, Mr. Hubbard testified that he did not recall sending the email or receiving a response and does not remember clicking on the hyperlinks in the email that would have led him to the patent in question. (*Id.* (citing Tr. at 2809:12-2810:1).) Similarly, PTX-1335, the email from Devin Redmond to Mr. Hubbard and Ramon Peypoch, does not indicate that Websense was considering a cross-license with Finjan "to get around patent issues," but instead only refers to the possibility of "offer[ing] strategic investment into CP Secure to get their patent rights for streaming scanning to get around Trend patent," not at issue here. (*Id.* (citing PTX-1335).)

Further, contrary to Finjan's assertion in its Opening Brief in Support of JMOL that "Websense's Board of Directors had discussions about Finjan and was concerned about infringing Finjan's patents," Mr. Hubbard actually stated that "[t]here were discussions about [Finjan] on the board. There was also discussions about them licensing some of our technology." (*Id.* (citing Tr. at 2823:16-21).) In fact, Mr. Hubbard testified that Websense's Board discussed licensing its URL filtering technology to Finjan and stated that he was "not particularly" interested in Finjan's patents. (*Id.* (citing Tr. at 2820:10-21).) Additionally, Websense CEO, John McCormack, testified that Websense never had access to any of Finjan's confidential information and "absolutely" did not believe that it infringed Finjan's patents. (*Id.* (citing Tr. at 2662:6-11, 2663:5-9).) Finally, in response to other evidence presented and to which Mr. Hubbard and Mr. McCormack responded, Websense details that: (1) PTX-1326, "Pre-emptive Web Security: Keeping Two Steps Ahead of the Treats," written by Mr. Hubbard, does not identify any specific Finjan patent and suggests nothing more than that Websense might investigate Finjan's patents (*Id.* (citing PTX-1326 at WEBS 00233330); (2) PTX-1397, the email from Mr. Hubbard to Mr. McCormack, does not relate to the '194 Patent; and (3) Mr. Hubbard testified that he only knew about one Finjan patent when he wrote the email and that patent related to client-side sandboxing technology, not the inventions claimed in the '194 Patent. (*Id.* (citing Tr. at 1310:16-1311:12).)[30]

At trial, the jury was presented with testimony from Mr. Hubbard and Mr. McCormack and was in a position to evaluate their credibility and consider the evidence. The court concludes, based on the evidence presented at trial and recited above, that the jury, if it found Mr. Hubbard and Mr. McCormack credible, could have reasonably found that Finjan did not satisfy the subjective prong and, therefore, there was no willful infringement. Indeed, it is the province of the jury to weigh such evidence and determine the credibility of witnesses. The jury's conclusion on this prong, coupled with the finding that there was no objectively-high likelihood of infringement based on the defendants' invalidity arguments, must result in denial of Finjan's JMOL motion.

[30] The court notes its agreement with Finjan that Websense cannot, as it attempts to do in its Brief in Opposition to JMOL, assert a constructive notice argument at this stage. Specifically, Websense contends that "Finjan's argument that Websense had notice prior to [June 6, 2008] from Finjan's product marking fails because marking creates at most a 'factual dispute as to constructive notice' that is not appropriate for resolution as a matter of law." (D.I. 808 at 15 n.7.) However, as Finjan correctly notes, Websense did not challenge Finjan's markings at trial, such that there can be no reasonable factual dispute on the issue. (D.I. 821 at 9.) In addition, Websense and the other defendants withdrew their initially proposed jury instruction on marking after Finjan's witnesses testified. (*Id.* (citing Tr. at 532:10-18, 655:4-665:2, 660:10-661:15).) Thus, because the jury was never charged with instructions regarding constructive notice, the court will not address Websense's contention that there is a factual dispute.

C. Websense's Motion for Attorney's Fees

Websense filed a Motion for an Award of Attorney's Fees and Expenses. (D.I. 762.) In support of its motion, Websense contends that Finjan: (1) accused two of its technologies—Uniform Resource Locator ("URL") filtering and RTSS—of infringement, despite knowing that neither could infringe[31]; (2) asserted method claims based solely on Websense's sales of products with no allegations, let alone evidence, of contributory infringement or inducement of infringement, increasing Websense's litigation costs; (3) improperly relied on the Entire Market Value Rule ("EMVR"), which was objectively baseless as a matter of law and was contradicted by Finjan's own experts; (4) had no reasonable basis to allege infringement under the doctrine of equivalents; and (5) acted in subjective bad faith by granting fact witnesses a stake in the outcome of the case and by failing to preserve evidence relating to the litigation after it knew of its duty to preserve such evidence.

In deciding whether to award attorney's fees, the court must undertake a two-step inquiry. *Interspiro USA, Inc. v. Figgie Intern. Inc.*, 18 F.3d 927, 933 (Fed. Cir. 1994). First, the court "must determine whether there is clear and convincing evidence that the case is 'exceptional.'" *Id.* (quotation omitted). Second, the court must decide whether "an award of attorney fees to the prevailing party is warranted." *Id.* Exceptional cases include: "inequitable conduct before the PTO; litigation misconduct; vexatious, unjustified, and otherwise bad faith litigation; a frivolous suit or willful infringement." *Epcon Gas Sys., Inc. v. Bauer Compressors, Inc.*, 279 F.3d 1022, 1034 (Fed. Cir. 2002) (citation omitted).

[31] Websense asserts that Finjan knew that its URL could not infringe the '194 Patent because it had licensed URL filtering from Websense for sale in its products. Websense also argues that Finjan learned during discovery that RTSS did not infringe because Finjan's own experts opined that signature-scanning cannot infringe the '194 Patent. (D.I. 763 at 6-13.)

An award of attorney fees under § 285 is not intended to be an "ordinary thing in patent cases," and should be limited to circumstances in which it is necessary to prevent a "gross injustice" or bad faith litigation. *Forest Labs, Inc. v. Abbott Labs.*, 339 F.3d 1324, 1329 (Fed. Cir. 2003); *see also Aptix Corp. v. Quickturn Design Sys., Inc.*, 269 F.3d 1369, 1375 (Fed. Cir. 2001) (affirming an award of attorney fees under § 285 for the "extreme misconduct" of falsifying evidence); *Beckham Instruments, Inc. v. LKB Produkter AB*, 892 F.2d 1547 (Fed. Cir. 1989) (affirming an award under § 285 following repeated violations of a permanent injunction and a district court finding of a "strategy of vexatious activity").

Having reviewed the parties briefing in connection with Websense's motion, the record before it, and the applicable law, the court will deny Websense's request for an award of attorney's fees. First, and with regard to Websense's assertions that Finjan improperly brought infringement claims against its URL and RTSS technologies despite knowing that they did not infringe, the court finds that the filing of these claims does not warrant an attorney's fees award. With respect to the URL infringement claims, Finjan initially brought allegations of infringement against Websense's Web Filter and Web Security products based on what it asserts to be a good faith belief that the products shared the same code base as the gateway products. (D.I. 774 at 6.) Finjan ultimately withdrew these allegations on March 8, 2012, after a February 7, 2012 deposition of Mr. Hubbard, during which it was revealed that these products do not include the same product code found in the gateway products. (*Id.*)

Moreover, Websense's claim that Finjan should have known that the products did not infringe before the completion of discovery because Finjan licensed the "SurfControl" URL database from Websense, does not persuade the court that Finjan acted in bad faith. As Finjan notes in its Brief in Opposition, the SurfControl URL database was a "legacy database"

Websense acquired from another company and was never an accused product or at issue because no Websense product used SurfControl URL. (*Id.*) Moreover, Finjan licensed access to the URL database, not the program code for the products. (*Id.*) Thus, it is not clear to the court that Finjan knew what program code was included in Websense's products before it completed discovery.

Further, and with regard to Websense's RTSS technology, Finjan put forth expert testimony, numerous Websense documents, source code, and deposition testimony describing the operation of the accused products in support of its infringement argument. Although Dr. Vigna did testify that the '194 Patent does not cover traditional "fingerprint" signatures, the technology that he discussed uses specific signatures to match a single malicious Downloadable. (*Id.* at 4-5.) Dr. Medvidovic also testified that the accused Websense gateway products receive a Downloadable, apply rules which identify different function cells or operations within the Downloadable, and then block or allow the Downloadable based on the intent of the Downloadable and the corresponding security policy. (*Id.* at 5.) Indeed, Finjan presented expert testimony, which, if the jury found the opinions to be credible, could render the Websense products covered by the asserted claims. Thus, although the jury found noninfringement, the court is not persuaded that Finjan's pursuit of this claim rises to litigation tactics or bad faith worthy of attorney's fees.[32] *See iLOR, LLC v. Google, Inc.*, 631 F.3d 1372, 1377 (Fed. Cir. 2011) (noting that infringement is "often difficult to determine" and therefore an infringement action is not "unreasonable in terms of [§ 285] if the infringement can reasonably be disputed").

Second, and in response to Websense's contention that Finjan's method claims against it were unfounded, Finjan asserts that these claims were based on Websense's testing and use of

[32] The court notes that it considers each of Websense's arguments alone and in combination, taking into account whether each individually or combined amounts to wrongful litigation conduct or bad faith rising to support an award of attorney's fees.

the accused products. (D.I. 774 at 9.) The Federal Circuit has established that testing and use is sufficient evidence to prove infringement of a method claim. *See Linear Tech. Corp. v. In't Trade Comm'n*, 566 F.3d 1049, 1062 (Fed. Cir. 2009). Here, Finjan identified evidence that Websense uses and tests its products, directly practicing the asserted method claims. In addition, Dr. Medvidovic testified that Websense's accused products infringe the asserted method claims and computer-readable claims and that this testing of products occurs in the United States. (D.I. 774 at 9-10.) As one example, Dr. Medvidovic testified that he reviewed deposition testimony from Websense engineers and executives indicating that Websense tested the Websense Web Security Gateway products. Consequently, the court does not find Finjan's claims that Websense infringed the asserted method claims to be brought in bad faith or objectively baseless.

Third, the court also finds that Finjan's allegations of infringement under the doctrine of equivalents do not warrant an award of attorney's fees. Specifically, Dr. Medvidovic provided testimony for each element of Claim 1 that the products containing RTSS technology performed substantially the same function, in substantially the same way, to obtain substantially the same result as the claimed limitations. (*Id.* at 11 (citing Tr. 1358:1-1360:21).) He provided similar testimony for the other remaining claim elements. In fact, the parties stipulated, with respect to Dr. Medvidovic's testimony, that to conserve time, he would only testify regarding the doctrine of equivalents for Claim 1 and then for the remaining claims he would testify that Websense infringes in the same fashion. (*Id.* at n.11 (citing Tr. at 1318:18-1319:12).) Websense was also denied the opportunity to file a motion for summary judgment on this issue. *See Medtronic Navigation, Inc. v. BrainLAB Medizinische Computersysteme GmbH*, 603 F.3d 943, 954 (Fed. Cir. 2010).

Fourth, the court similarly rejects Websense's argument that attorney's fees should be granted based on Finjan's use of the EMVR, because it does not find Finjan's use of this rule to be objectively baseless. The court held a *Daubert* hearing and ordered rounds of briefing on the question of whether the EMVR could be introduced and, ultimately, did not exclude presentation of the Rule in its entirety. Rather, the court modified Dr. Parr's proposed definition of the "smallest salable patent practicing unit." (D.I. 774 at 13 (citing Tr. at 932:10-24).) In support of applying EMVR, Finjan relied on: Dr. Parr's opinion that the specific accused technology was needed to provide complete, effective protection against malware, which was the basis of customer demand; its past licenses to the '194 Patent; and industry reports from third party market analysts. (*Id.* at 16.) Thus, Finjan's attempted application of the rule was not objectively baseless.

Finally, Websense's argument that Finjan engaged in litigation misconduct that merits an award of attorney's fees is unpersuasive in view of the applicable standard. With respect to Websense's assertion that Finjan wrongfully and improperly gave fact witnesses a financial stake in the outcome, Finjan responds that it no longer has active employees and, therefore, employed Mr. Touboul, Finjan's founder and the named inventor on multiple Finjan patents, and Mr. Ben-Itzhak, Finjan's former Chief Technology Officer and named inventor on multiple patents, to provide information regarding the company's patent portfolio and other matters. (*Id.* at 17.) Mr. Touboul's agreement specifies multiple services, including providing advice regarding Finjan's intellectual property portfolio and reexaminations. (*Id.*) Mr. Ben-Itzhak's consulting agreement also specifies providing multiple services, such as working with other employees, consultants, or service providers to commercialize Finjan's intellectual property and assist with questions related to Finjan's patent applications. (*Id.*)

Thus, Finjan argues that these fact witnesses were not signed as consultants simply to testify in this litigation. For instance, Mr. Ben-Itzhak has been paid by Finjan for consulting services since he left the company in 2009, advising on many technical patent matters, and both he and Mr. Touboul are still employed after the litigation ended. (*Id.*) Neither consultation agreement made payment for services contingent on the outcome of the litigation or the content of their testimony and neither has control over how cash proceeds are distributed to shareholders by the Board. (*Id.* at 17-18.) Moreover, both witnesses were questioned on cross-examination as to their consulting work for Finjan and both testified that they were not being paid for their testimony and had no stake in the litigation outcome. (*Id.* at 18.) Finjan further asserts that, under the ABA Standing Committee on Ethics and Professional Responsibility, paying a fact witness for his or her time is appropriate so long as that payment is not being made for the substance of that individual's testimony. (*Id.*)

Additionally, and with regard to Websense's assertion that Finjan destroyed documentation relevant to the litigation, Finjan argues that Websense has presented no evidence that it "destroyed" documents or failed to preserve documents related to this case. (*Id.* at 19.) Finjan notes that it searched for and produced non-privileged documents in response to the defendants' document requests and, ultimately, turned over thousands of documents, including all documents produced in the prior *Secure Computing* litigation, financial statements, technical documents, white papers, source code, product specifications, board presentations, marketing documents, licenses, competitive analyses, product manuals, stock purchase agreements, emails, invoices, and corporate documents. (*Id.*) In response to multiple subpoenas, M86 also produced documents to Websense, including stock purchase agreements with Finjan, financial statements, competitive analyses, and license agreements. Moreover, Finjan notes that the document

Websense cites to show that Finjan contemplated litigation against Websense since 2008,[33] was a board meeting presentation stating that Finjan wanted to "enforce patents against any active infringers" and stated that Websense was interested in an opportunity to engage in a strategic combination with Finjan. (*Id.* at 20.) In light of this evidence, Finjan asserts and the court agrees, that Websense has not clearly and convincingly demonstrated that Finjan destroyed or failed to preserve documents in anticipation of this action or that it improperly compensated fact witnesses.

In view of the foregoing, the court concludes that Finjan's conduct in this case does not rise to a level of bad faith or vexatious litigation that warrants an award of attorney fees and costs. While the parties in this litigation certainly engaged in "hardball" litigation tactics throughout the pendency of this litigation, none of their conduct was "exceptional" in that regard. *See Forest Labs., Inc. v. Ivax Pharms., Inc.*, No. 03-891-JJF, 2008 U.S. Dist. LEXIS 14623, at 6-7 (D. Del. Feb. 26, 2008) (concluding that "hard-fought" litigation does not necessarily constitute "vexatious or bad faith litigation" for purposes of awarding attorney fees under § 285). For the most part, the parties defended their respective positions throughout this litigation in apparent good faith and the court does not find evidence in the record sufficient to support the assertion that Finjan acted in subjective bad faith or conducted its litigation in a manner warranting attorney fees. The court finds, therefore, that Websense is not entitled to an award of attorney fees and costs in this case.

D. Finjan's Motion for a New Trial

In addition to its renewed motions for JMOL, Finjan also filed a Motion for a New Trial. (D.I. 773.) Finjan bases its motion on three grounds: (1) substantial errors in the admission and

[33] Websense asserts that Finjan transferred its assets to M86 in November 2009 and only kept documents that its counsel deemed related to its patents. (D.I. 763 at 20.) Websense further argues that Finjan transferred all other documents to M86 and did not retain any copies of such documents. (*Id.*)

rejection of evidence and in the jury instruction unfairly influenced the jury verdict; (2) the jury verdict of noninfringement and invalidity was against the clear weight of the evidence; and (3) the jury verdict was facially inconsistent. (*Id.*) In consideration of the parties' briefings in connection with Finjan's motion, the evidence in the record before it, and the relevant law, the court will deny Finjan's Motion for a New Trial. The court addresses each of Finjan's arguments in turn below.

First, Finjan contends that the errors made in the admission and rejection of evidence as well as in instruction to the jury includes: (1) excluding Dr. Vigna's testimony regarding his review of binary and assembly language code for the asserted prior art; (2) instructing the jury to deem the prior art source code as evidence of how the asserted prior art operates; and (3) excluding evidence and argument that Sophos' evidence regarding the availability of SWEEP-InterCheck was flawed and unreliable. (D.I. 789 at 3.) Finjan argues that these alleged errors, individually and, particularly, in combination: "seriously compromised" its validity rebuttal case because "it prevented Finjan from showing the jury substantial deficiencies in [the defendants'] foundational evidence"; and impacted the credibility of Finjan's technical experts, "leaving them open to inappropriate and unwarranted criticism regarding the use of source code," which may have impacted the validity and infringement verdicts. (*Id.*) Finjan asserts that these errors were, particularly with respect to its validity case, "so prejudicial that denial of a new trial would be 'inconsistent with substantial justice.'" (*Id.* (citing *Mondzelewski v. Pathmark Stores, Inc.*, C.A. No. 96-359 MMS, 2000 WL 654137, at *20 (D. Del. Mar. 20, 2000) (quotation and citations omitted)).)

Regarding Dr. Vigna's excluded testimony about his review of binary and assembly language code, Finjan asserts that the court excluded this testimony because it believed that Dr.

Vigna did not testify about this topic on his direct examination or cross-examination, when in fact he had. Specifically, Finjan states that Dr. Vigna testified that he looked at the executable binary and assembly code for the asserted prior art to understand "what functions are called and what is done by the program, without looking at any source code." (*Id.* at 3-4 (citing Tr. at 3030:3-3031:11).) Dr. Vigna also testified on direct that binary code is instructive in determining how a product actually works because that code is a set of instructions that a computer actually follows, as opposed to source code, which is not executed by a computer and, instead, is used to generate assembly and binary code. (*Id.* at 4 (citing Tr. at 3140:9-14 ("the very ultimate way to understand how the program works is to look at the binary code because the same source code can actually be compiled into different binary code, and therefore, the only real way to know what gets executed is to look into the binary code")).) Finjan notes as well that on cross-examination Dr. Vigna testified, in response to a question as to whether source code is "a very important set of instructions on how the program operates":

> Right. But what I am saying is the very ultimate way to understand how the program works is to look at the binary code because the same source code can actually be compiled into different binary code, and, therefore, the only real way to know what gets executed is to look into the binary code. . . . Actually, I can go to a lower level, which is using debuggers and disassemblers to look actually at how the binary code operates.

Tr. at 3140:7-14, 3147:14-19.

Finjan contends that the court's exclusion of this testimony severely prejudiced its case, particularly because: Sophos' counsel tried to discredit and admonish Dr. Vigna for not reviewing the source code (*id.* (citing Tr. at 3139:21-3140:6, 3143:3-3144:8)); Finjan was not able to rehabilitate Dr. Vigna's testimony and expound on his statement during direct examination that the binary code "was a better source of material" (*id.* (citing Tr. at 3159:15-17)); and the defendants highlighted that Dr. Vigna did not review the source code in their closing arguments (*id.* (citing Tr. at 3331:6-9, 3339:11-21, 3346:4-5, 3361:8-19, 3362:23-3363:16-23)). Thus, Finjan asserts that the court's exclusion of Dr. Vigna's testimony was incorrect because he did testify as to binary code on direct as well as on cross-examination.

The court disagrees with Finjan's assertion that the exclusion of Dr. Vigna's testimony on this issue warrants a new trial. As the defendants note in their Brief in Opposition to Finjan's Motion for a New Trial, throughout the trial, the parties focused on the source code of the accused products and prior art products as the best evidence of how the products operate. (D.I. 811 at 3-4.) Indeed, during its opening statement, Finjan's counsel explained that "[s]ource code, to computer scientists, that is the good stuff. That is the DNA of what is happening." (*Id.* at 4 (citing Tr. at 339:16-18).) Likewise, Finjan's infringement expert testified that source code is the DNA of the system in question. (*Id.* (citing Tr. at 725:2-5 ("I relied on source code, which is kind of, as it was characterized earlier in the proceedings, the DNA of the system in question.")).) The defendants' invalidity experts also focused on the source code of the prior art products. (*Id.* (citing Tr. at 2097:12-20, 2102:3-2105:3, 2128:22-2129:3, 2129:16-2130:13).)

However, because Finjan's validity expert, Dr. Vigna, founded and works for a company that competes with the defendants, he was unable to sign the Protective Order and, therefore, could not review the source code for the asserted prior art products or the accused products. (*Id.*) To compensate for this inability to review the source code of the prior art products, Dr. Vigna testified on direct examination that he reviewed the executable code. Specifically:

> Q: When you say you looked at the program itself, did you look at the assembly language or anything along those lines?
>
> A: I looked at the executable code because, of course, I had no access to the source code. And in order to understand to the best of my knowledge what the program was doing, I opened the manual—the assembler and look at the assembly.

> Q: Would you describe generally speaking what is assembly code?
>
> A: Programs, when we buy them and we install them in our system, most of the time are in binary form. So they are sequences of ones and zeros. These sequences are loaded into memory and executed. And every single little sequence represents an instruction. If you look at them as sequences of ones and zeros, it is super-boring and almost impossible to understand what's really going on. But there is a small increase in the level of abstraction called assembly code in which the code that is being executed at the machine level is actually presented in a way that is human-readable. So you can see, for example, if there is an instruction that jumps to a certain address, if a certain function is called. By that you can understand how the program operates.
>
> Q: Did you do anything to confirm that your understanding of how NAV 95 operates was correct, at least according to the source code?
>
> A: So I ran the program, so I saw how it operates, how it scans files. I looked at the assembly, of course, to understand what functions are called and what is done by the program, without looking at any source code.

Tr. at 3030:7-3031-11. As noted above, Dr. Vigna then testified on cross-examination, in response to a question as to whether source code is important in assessing how a program operates, that the "very ultimate way to understand how the program works is to look at the binary code" and, further, that "the only real way to know what gets executed is to look into the binary code." *Id.* at 3140:7-14, 3147:14-19.

On redirect, Finjan's counsel asked Dr. Vigna, "[n]ow, you mentioned binary code in connection with SWEEP/InterCheck, and you thought this was a better source of material. Why is that?" (D.I. 811 at 5 (citing Tr. at 3159:15-3160:1).) The court directed the parties to sidebar and stated: "It's not my job to judge this witnesses' credibility, but I am not going to let him confuse this jury with a discussion about binary code. No expert in this case has talked about binary code, including this gentlemen on his direct testimony." Tr. at 3159:15-3160:1.

As is clear from the court's statement quoted above, it excluded Dr. Vigna's testimony on binary code so as to prevent juror confusion and because, on direct examination, Dr. Vigna provided only conclusory testimony that he reviewed the binary and assembly code for products such as NAV 95. During his direct testimony, Dr. Vigna did not provide any details concerning his alleged review of the binary and assembly code and did not testify—contrary to the statement in Finjan's question on redirect—that these materials were better or more meaningful than source code. Rather, the only statement that Dr. Vigna made to this affect was in response to a question on cross-examination related to source code and, in his reply, Dr. Vigna stated simply that reviewing binary code "is the very ultimate way to understand how the program works" and "to know what gets executed." Tr. at 3140:7-14.

At no point in his direct or cross-examination testimony did Dr. Vigna provide any specific or meaningful testimony as to his analysis of the binary code. Thus, it was proper for the court to exclude Dr. Vigna's testimony on whether binary code is better than source code, as this testimony would have been unreliable, misleading, and potentially confusing to the jury. Indeed, and as noted above, throughout trial the parties and all other technical experts addressed only source code, not binary code. The only discussion of binary code in the record is the testimony passages the court cites above. This direct examination testimony and Dr. Vigna's cross-examination response were insufficient to establish whether binary code is on par with or more meaningful than, source code. Notably, Finjan's counsel did not submit an offer of proof at sidebar for the testimony that Dr. Vigna would have offered and did not explain the relevance of such testimony. The court, therefore, precluded redirect examination on binary code to prevent confusion and did so properly.[34]

[34] Moreover, even if the court did err in excluding this testimony, which it did not, the court finds that Finjan has not shown that the error was so prejudicial that denial of a new trial would be inconsistent with substantial justice. Indeed, the jury could have found invalidity based on the separate prior art references Symantec introduced, which the court discussed in greater detail above. *See Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000) ("in entertaining a motion for judgment as a matter of law, the court should review all of the evidence in the record"). The jury was presented with information regarding all of the relevant facts on which Dr.

The court further notes that Finjan presented no legal or technical support for the proposition that binary code is more relevant than source code or that Dr. Vigna "performed a more relevant and deeper analysis by examining the actual machine executable code." (D.I. 789 at 5.) On direct, Finjan did not seek to elicit any meaningful testimony regarding the details of the binary or machine code for any prior art reference, thus undercutting this argument in its entirety. In fact, as the defendants note, Finjan presumably did not elicit such testimony because Dr. Vigna's rebuttal report was devoid of any substance regarding this issue and any testimony would likely have been inadmissible on this point.

Second, Finjan maintains that the jury should not have been instructed to assume that source code correlated to alleged prior art and that this instruction "eviscerated one of Finjan's major validity arguments" because Finjan had repeatedly argued that the defendants had failed to lay a proper foundation establishing that the source code corresponded to software products available in the United States before the priority date. (*Id.* at 5-6.) Specifically, Finjan takes issue with the court's instruction, during Finjan's closing argument, that:

> I think [Mr. Andre] has made a statement, perhaps unintentionally, that might be misleading to you, I want to give you a brief bit of guidance, as to source code and what he just said. The defendants in this case relied on products as prior art, the products as prior art. They relied on source code, and the witnesses, the experts talked about source code, to demonstrate how the prior art products work and therefore demonstrate the invalidity, in their view, of the particular Finjan patents that are at issue.

Tr. at 3415:12-24. Finjan argues that this instruction was in error because: Dr. Vigna was precluded from offering his analysis of assembly and binary code to rebut the defendants' "incorrect claim that his validity analysis was flawed for lack of source code review"; "the [c]ourt's comments regarding the relevance of source code (in the context of Finjan's discussion

Vigna relied in forming his opinions and could have properly decided to believe the competing testimony of the defendants' experts.

of Dr. Vigna's analysis) effectively endorsed [d]efendants' incorrect claim that their invalidity experts had undertaken a more thorough and appropriate analysis"; and, as noted above, the instruction undermined Finjan's argument that the defendants had failed to lay a proper foundation for tying the source code to the asserted prior art. (D.I. 789 at 6-7.)

Considering this instruction in the context in which it was made, the court disagrees. Contrary to Finjan's assertion that the court instructed the jury to assume that the source code corresponded to the alleged prior art, and as is clear from the quoted passage below, the instruction was given in response to and to correct an assertion made by Finjan's counsel. Specifically, Finjan's counsel stated:

> [The defendants] all attack Dr. Vigna. Dr. Vigna didn't review the source code. Why didn't he review the source code? *Because the law tells him not to*. He was a validity expert and a tutorial expert. It states in Section 4.3 again that the references defendants have asserted are prior art. Defendants must prove on a claim-by-claim basis that it is accessible to the public or commercially exploited in the United States. *He was required to rely on public information. Source code is not public information.* That was what the law requires. And he got beat up for it by all three advocates.

Tr. at 3413:6-18 (emphasis added). Because the prior art the defendants asserted was the products themselves, Finjan's statement was incorrect as a matter of law and misleading to the jury. Rather, it was appropriate for the defendants' experts to rely upon the source code to explain how the products worked. *See Touchcom, Inc. v. Bereskin & Parr*, 790 F. Supp. 2d 435, 453-54 (E.D. Va. 2011) (rejecting the argument that a product is not prior art because the public would not have been able to see its source code); *Lab. Skin Care, Inc. v. Limited Brands, Inc.*, 2011 WL 4005444, at *5 (D. Del. Sept. 8, 2011) (concluding that "the offered product is in fact the claimed invention may be established by any relevant evidence, such as memoranda, drawings . . . and testimony of witnesses" (citation omitted)).

Recognizing this, the court explained to the jury that the defendants had "relied on source code, and the witnesses, the experts talked about source code, to demonstrate how the prior art product worked." Tr. at 3415:19-24. This correction did not undermine "Finjan's argument that [d]efendants failed to lay a proper foundation connecting the source code to the asserted prior art," as the court did not instruct the jury to assume anything other than the fact, under the law, it was appropriate for the defendants to use source code and witnesses testimony to try to establish how the asserted prior art worked. (D.I. 789 at 6-7.) The court made no statements endorsing the defendants' representations regarding the prior art. Notably, Finjan did not argue during its closing argument that the defendants had failed to lay a proper foundation connecting the source code to the prior art. Moreover, it was appropriate for the court to issue this instruction because Finjan agreed that it would not raise any issues concerning the enablement of the prior art software products. (D.I. 672 at 1.)

Finjan also argues that the court's instruction prevented it from offering testimony regarding Dr. Vigna's analysis of assembly and binary code. (D.I. 789 at 6.) However, during the sidebar, the court clearly explained: "I think it is very disingenuous of you to argue to this jury that source code is not publicly available. We all know that. These defendants have clearly relied on these products." Tr. at 3414:12-15. Thus, Finjan understood that the court's instruction had no relation to Finjan's proffering of any testimony regarding Dr. Vigna's analysis of assembly and binary code.

Third, Finjan contends that it should have been permitted to introduce evidence showing that Sophos' SWEEP-InterCheck evidence was unreliable. Specifically, Finjan states that it was improperly prohibited from showing the jury: (1) that the floppy disks that Sophos presented at trial did not correspond to the asserted versions of SWEEP-InterCheck and were not prepared until late 1996, even though Mr. Klausner had incorrectly testified that the disks were shipped "in 1995 and prior"; (2) the CD ROMs Sophos relied upon as containing the purported prior art had a copyright and build date of no earlier than 2011 and, therefore, cannot be evidence of the availability of SWEEP-InterCheck in 1996; and (3) that Mr. Klausner's demonstrative programs had file modification dates ranging from 1990 to 1995, even though he testified that he did not prepare these demonstratives until recently, suggesting that the system clock on his computer had been set back to that time period, and calling into serious question the verifiability of other times and date data upon which Sophos relied. (*Id.* at 7-8.)

Finjan argues the exclusion of this evidence severely prejudiced its case because a central feature of its response to Sophos' invalidity case was that Sophos did not provide clear and convincing evidence that the purported combination of Sweep 2.72 and InterCheck 2.11 was available in the United States before the priority date and that Sophos did not reliably demonstrate the actual functionality of the purported combination. (*Id.* at 8.) Based on the record, the court cannot agree.

Specifically, during trial Sophos presented live testimony and documentary evidence that SWEEP-InterCheck was available in the United States before the priority date. During trial, Finjan had the opportunity to cross-examine Sophos' founder, Dr. Hruska, regarding this issue, but did not sufficiently do so. In particular, Finjan failed to ask detailed questions about SWEEP 2.72 or InterCheck 2.11, which was the subject of Dr. Hruska's testimony. Instead, Finjan inquired as to whether SWEEP and InterCheck were sold independently, as well as the place the first sale of the product was made. Finjan did not ask any questions about any specific version of the product. *See* Tr. at 2370:9-19. Based on this line of questioning, Dr. Hruska testified, consistent with his past testimony, that InterCheck was always sold with SWEEP, and that the first sale occurred in 1993. *Id.* Finjan did not ask any other questions regarding dates.

Having failed to cross-examine Dr. Hruska on this issue at trial, Finjan cannot now seek to rectify this failure through a new trial. *See GNB Battery Techs., Inc. v. Exide Corp.*, 876 F. Supp. 582, 604 (D. Del. 1995), *aff'd*, 78F.3d 605 (Fed. Cir. 1996) (denying a motion for a new trial made on grounds that the expert opined on issues beyond the scope of his qualifications because the defendants failed to take advantage of the opportunity to conduct cross examination on those issues); *see also Symbol Techs. Inc. v. Opticon, Inc.*, 935 F.2d 1569, 1576 (Fed. Cir. 1991) (a party choosing not to cross examine a witness on an issue cannot later "recoup for its failed litigation strategy []"). Thus, Finjan's assertion that it was precluded from rebutting Sophos' evidence that SWEEP 2.72 and InterCheck 2.11 were available in the United States before the priority date is not persuasive.

Moreover, Finjan argues that various demonstratives that Sophos used to aid the jury's understanding of SWEEP-InterCheck as prior art improperly influenced the jury because Finjan was not allowed to show information regarding those demonstratives. (D.I. 789 at 7-8.) However, Finjan had the opportunity to cross-examine Mr. Klausner, who presented the floppy disk, CD ROMs, and demonstratives, and did not do so. Therefore, for the same reasons advanced in connection with Finjan's failure to cross-examine Dr. Hruska, Finjan cannot remedy its failure to explore this issue with a new trial.

Finjan also argues in its Reply that it was not required to cross-examine Dr. Hruska about Sophos' source code, as the defendants suggest, because the excluded arguments relate to Mr. Klausner's invalidity presentation. Thus, Finjan argues that it should have been allowed to use this evidence during its rebuttal case on invalidity. Tr. at 2467:17-25. Indeed, Finjan did raise the issue of presenting this evidence through Dr. Vigna's testimony and the court engaged in a lengthy discussion with the parties as to the inclusion of this evidence.[35] *Id.* at 3000:17-3013:6, 3172:10-3173:5. During this discussion, Finjan asserted that Sophos did not provide it with copies of the floppy disks and CR ROMs before trial and did not receive them until the trial began, at which time it recognized the inconsistent dates. *Id.* at 3004:16-21, 3006:1-22. Based on these inconsistent dates, Finjan argued that it should have the opportunity to introduce this fact to the jury so that the jury could consider whether the program versions shown on the machine at trial corresponded to the dates represented. *Id.* at 3004:22-3006:22.

Sophos, however, responded that the floppy was simply a "dummy" and that the dates Sophos represented with respect to the version on the machine were accurate, rejecting Finjan's allegation to the contrary. *Id.* at 3009:2-9. In precluding Dr. Vigna from testifying as to the dates on the floppy disks, CR ROMs, and demonstratives, the court explained:

> I have got officers of the Court here who have made representations that, if proven false, would be sanctionable. I have to believe that we are all honorable people here and that I can rely on the representations that are being made concerning this factual dispute. This is a dispute over what you say is on the machine and what Sophos says is on the machine. . . . We are ending this discussion. I have ruled concerning Dr. Vigna's ability to talk about source code. I think that should be clear. That's the end of that.

Tr. at 3009:11-24. For the reasons articulated during that ruling, the court finds that its exclusion of Dr. Vigna's testimony was proper. Finjan did not cross-examine Mr. Klausner as to the dates on the floppy disks and CD ROMs or dates displayed in the demonstrative when it had the opportunity to do so and the court properly relied on the representations made by Sophos'

[35] Finjan also notes that it raised these topics in its proffer. *See* Tr. at 3172:10-3173:5.

counsel that the items in question were "dummy" versions and not the versions on the machine. A new trial is not warranted.[36]

Fourth, Finjan claims that it is entitled to a new trial because, as detailed more fully in its submissions in connection with its renewed motions for JMOL, the jury verdict was against the weight of the evidence. On this point, Finjan and the defendants highlight the arguments they advanced in their JMOL briefing. Because the court has presented its examination of the record with respect to Finjan's renewed requests for JMOL above, it does not restate those findings here. In sum, for the reasons stated above, the court finds that jury verdict of both invalidity and noninfringement was not against the clear weight of the evidence in this case. Consequently, a new trial is not warranted on this ground.

Finally, Finjan contends that the court should grant a new trial because the jury verdict was facially inconsistent, "proving that the jury was confused as to the undisputed facts, the law[,] or both." (*Id.* at 9.) With regard to Sophos, Finjan argues that the jury could not have logically concluded that the asserted claims were both invalid and not infringed. Specifically, Finjan notes that during trial Sophos' defense was based on the theory that earlier versions of its accused product, which Sophos alleged operated in the same way as the accused products, were prior art to and fell within the scope of the asserted claims. (*Id.*) As discussed above in connection with Finjan's JMOL motion as to Sophos, Finjan notes that Sophos' counsel made this point expressly in his closing argument.[37] (*Id.* at 9-10.)

Finjan further asserts that the same is true with respect to Websense, as Websense counsel stated in his closing: "If you find that the '194 Patent is invalid, it means that that patent

[36] As the defendants note, Finjan could have had an expert analyze the SWEEP-InterCheck source code. Finjan did not and, as a result, was left to cross-examination of Sophos' witnesses. Finjan did not do so and cannot seek a new trial at this stage on that ground.

[37] *See supra* Section III.B.1.

and all the claims that are found invalid are invalid as to Websense, too. And that means that there could be no infringement." (*Id.* at 10 (citing Tr. at 3380:4-8).) This, Finjan argues, is inconsistent with the jury verdict form, which asked the jury to first determine infringement and then separately determine invalidity. Thus, Finjan contends that the "jury may have found (incorrectly) that the asserted claims were invalid in view of Sophos' prior art and then followed the incorrect instruction of Websense's counsel and improperly found no infringement by Sophos and the other defendants for that reason alone." (*Id.* at 10-11.) Finjan notes that it had requested that the verdict form direct that the jurors identify any specific reference found to render a patent anticipated or obvious and that only the defendant that presented the evidence be named in the verdict question. (*Id.* at 11.) The court, however, had the parties file a joint verdict form and removed the question asking jurors to identify which reference was found to be anticipatory or obvious. (*Id.*) Therefore, Finjan asserts that it is not possible to determine what or whose evidence the jury used to determine that the patent was invalid.

On this point, Finjan maintains that, under Third Circuit precedent, a new trial is warranted because, when a jury verdict is irreconcilably inconsistent on two points, "the appropriate remedy is ordinarily, not simply to accept one verdict and dismiss the other, but to order an entirely new trial." (*Id.* at 10 (citing *Calloway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1344-45 (Fed. Cir. 2009); *Comaper Corp. v. Antec, Inc.*, 596 F.3d 1343, 1355 (Fed. Cir. 2010)).)

Again, the court cannot agree. First, and with respect to Websense counsel's closing argument statement that a finding of invalidity "means that there could be no infringement," this statement was not an incorrect recitation of the law. Indeed, "an invalid claim cannot give rise to liability for infringement." *Medtronic, Inc. v. Cardiac Pacemakers, Inc.*, 721 F.2d 1563, 1583 (Fed. Cir. 1983). The Federal Circuit has also recognized that one cannot infringe an invalid patent as a matter of law. Importantly, Finjan failed to object to this statement at trial and, therefore, waived its claim to a new trial on this ground. *Murray v. Fairbanks Morse*, 601 F.2d 149, 152 (3d Cir. 1979) ("[F]ailure to object precludes [a party] from seeking a new trial on the grounds of the impropriety of opposing counsel's closing remarks." (citation omitted)); *Waldorf v. Shuta*, 142 F.3d 601, 629 (3d Cir. 1998) ("[I]t is clear that a party who fails to object to errors at trial waives the right to complain about them following trial."); *Matsushita Elec. Indus. Co., Ltd. v. Samsung Elecs. Co., Ltd.*, 2006 WL 3193982, at *14-15 (D.N.J. Nov. 2, 2006) (motion for a new trial denied on the ground that "counsel's argument to the jury telling them to analyze the invalidity issues before addressing the infringement issue" confused the jury, because the movant failed to object to this statement at trial).

The court further finds that its jury instruction and the jury's question during the deliberations regarding their duty to consider both infringement and invalidity make clear that the jury was not confused. Specifically, the court instructed the jury that it was to determine infringement as to each defendant, and then, after that deliberation was complete, determine if the asserted patents are invalid. *See* Tr. at 3230:20-3233:6. The court's instruction that the jury should determine infringement before determining invalidity cured any potential prejudice or confusion from Websense's counsel's statement. *See Mente Chevrolet Oldsmobile, Inc. v. GMAC*, 728 F. Supp. 2d 662, 679-80 (E.D. Pa. 2010) (denying a motion for a new trial based in part on alleged jury confusion resulting from the scope of expert testimony and noting that any confusion was cured by "an appropriate jury instruction"); *Klink v. Harrison*, 332 F.2d 219, 225 (3d Cir. 1964) (noting that there "is a presumption that a verdict is rendered in accordance with the instruction of the trial judge"). Moreover, the jury's question demonstrated that it was not confused, as it determined that none of the defendants infringed the patents-in-suit before assessing whether the patents were invalid. Specifically, the jury asked, "If the jury finds that Finjan has not proven infringement by any of the defendants, is it necessary to answer Verdict Question 7 through 8 [pertaining to invalidity]?" *See* Tr. at 3429:3-10. Thus, it is clear that the jury considered these two questions separately.

It is well established that it is the patentee's burden to prove infringement. Here, the jury found that Finjan did not meet this burden and the jury's verdict of noninfringement and invalidity was supported by sufficient evidence in the record. Absent proper support that the verdicts were inconsistent, which Finjan has not shown, the court cannot grant its request for a new trial on this ground.

The court further finds that the jury verdict form was, in fact, proper. Indeed, the jury was not required to identify the basis for invalidity or the specific prior art reference or references upon which it relied. The form was also consistent with other patent cases involving multi-reference invalidity arguments. *See, e.g., Cordance Corp. v. Amazon.com, Inc.*, 658 F.3d 1330, 1333 (Fed. Cir. 2011); *i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 845 (Fed. Cir. 2010). Notably, it is within the court's discretion to determine the content and structure of the verdict form. *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1248 (Fed. Cir. 2010). The court finds that it properly exercised this discretion here, and Finjan does not provide case support for its proposition that verdict form requires the level of specificity that Finjan advances. Notably, Finjan opposed the defendants' request to require a similar level of specificity in the verdict form as it relates to the alleged infringement. (D.I. 716 at 1; D.I. 725 at 1.)

In the Third Circuit, inconsistent verdicts "may constitute grounds for ordering a new trial . . . if 'no rational jury could have brought back the verdicts that were returned.'" *See Monaco v. City of Camden*, 366 Fed. Appx. 330, 331-32 (3d Cir. 2010) (citing *Mosley v. Wilson*, 102 F.3d 85, 91 (3d Cir. 1996)). Finjan has not demonstrated that the jury's verdicts were irreconcilably inconsistent, that the jury verdict resulted from its confusion as to the validity and infringement positions advanced at trial, or that the verdicts were irrational. To the contrary, as explained in the court's JMOL analysis above, the jury could have reasonably reached its decisions of noninfringement and invalidity based on substantial evidence in the record. Finjan also has not demonstrated that the jury was confused or that it should have been required to supply more specific information on the jury form. Thus, for the reasons set forth in this Memorandum Opinion, the court finds that a new trial is not warranted in this case.

V. CONCLUSION

For the reasons stated above, the court will deny all of the outstanding post-trial motions.

Dated: September 19, 2013

CHIEF, UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINJAN, INC.,)
)
Plaintiff,)
)
v.)
) C.A. No. 10-cv-593 (GMS)
SYMANTEC CORP., SOPHOS, INC.,)
and WEBSENSE, INC.,)
)
Defendants.)
)

ORDER

For the reasons stated in the accompanying Memorandum of the same date, IT IS HEREBY ORDERED that:

1. Finjan's Renewed Motions for Judgment as a Matter of Law (D.I. 770; D.I. 771; D.I. 772) are DENIED;
2. Finjan's Motion for a New Trial (D.I. 773) is DENIED; and
3. Websense's Motion for Attorney Fees (D.I. 762) is DENIED.

Dated: September 19, 2013

CHIEF, UNITED STATES DISTRICT JUDGE

US006092194A

United States Patent [19]

Touboul

[11] **Patent Number: 6,092,194**

[45] **Date of Patent: *Jul. 18, 2000**

[54] **SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES**

[75] Inventor: **Shlomo Touboul**, Kefar-Haim, Israel

[73] Assignee: **Finjan Software, Ltd.**, Netanya, Israel

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/964,388**

[22] Filed: **Nov. 6, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/030,639, Nov. 8, 1996.

[51] **Int. Cl.**^{7} **H04L 1/00**

[52] **U.S. Cl.** **713/200**

[58] **Field of Search** 395/187.01, 186; 713/200, 201, 202; 714/38, 704; 709/229

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,077,677	12/1991	Murphy et al.	395/10
5,361,359	11/1994	Tajalli et al.	395/700
5,485,409	1/1996	Gupta et al.	395/186
5,485,575	1/1996	Chess et al.	395/183.14
5,572,643	11/1996	Judson	395/793
5,623,600	4/1997	Ji et al.	395/187.01
5,638,446	6/1997	Rubin	380/25
5,692,047	11/1997	McManis	380/4
5,692,124	11/1997	Holden et al.	395/187.01
5,720,033	2/1998	Deo	395/186
5,724,425	3/1998	Chang et al.	380/25
5,740,248	4/1998	Fieres et al.	380/25
5,761,421	6/1998	van Hoff et al.	395/200.53
5,765,205	6/1998	Breslau et al.	711/203
5,784,459	7/1998	Devarakonda et al.	380/4
5,796,952	8/1998	Davis et al.	395/200.54
5,805,829	9/1998	Cohen et al.	395/200.32
5,832,208	11/1998	Chen et al.	395/187.01
5,850,559	12/1998	Angelo et al.	395/750.03
5,864,683	1/1999	Boebert et al.	395/200.79
5,892,904	4/1999	Atkinson et al.	395/187.01

OTHER PUBLICATIONS

Web page: http://iel.ihs.com:80/cgi–bin/iel_cgi?se...2ehts%26ViewTemplate%3ddocvie%5fb%2ehts, Okamato, E. et al., "ID–Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013–5194, Jul. 19, 1990, Abstract and pp. 1169–1170.

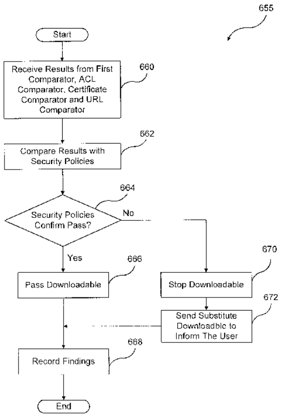
(List continued on next page.)

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Christopher Revak
Attorney, Agent, or Firm—Graham & James LLP

[57] **ABSTRACT**

A system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

68 Claims, 10 Drawing Sheets


655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
Security Policies Confirm Pass?
664
No
Yes
Pass Downloadable
666
Stop Downloadable
670
Send Substitute Downloadable to Inform The User
672
Record Findings
668
End

Plaintiff's Trial Exhibit
PTX-1
Case No. 10-CV-00593-GMS

OTHER PUBLICATIONS

"Finjan Announces a Personal Java ™ Firewall For Web Browsers—the SurfinShield™ 1.6", Press Release of Finjan Releases SurfinShield, Oct. 21, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software, Ltd., Jul. 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™"Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

"Company Profile Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavillion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Article published on the Internet, 7 pages.

Mark LaDue, "Online Business Consultant" Article published on the Internet, Home Page, Inc. 1996, 4 pages.

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, p 27, May 1990.

Norvin Leach et al, "IE 3.0 applets will earn certification", PC Week, v13, n29, p1(2), Jul. 1996.

Microsoft Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996.

Frequently Asked Questions About Authenticode, Microsoft Corporation, Feb. 1997.

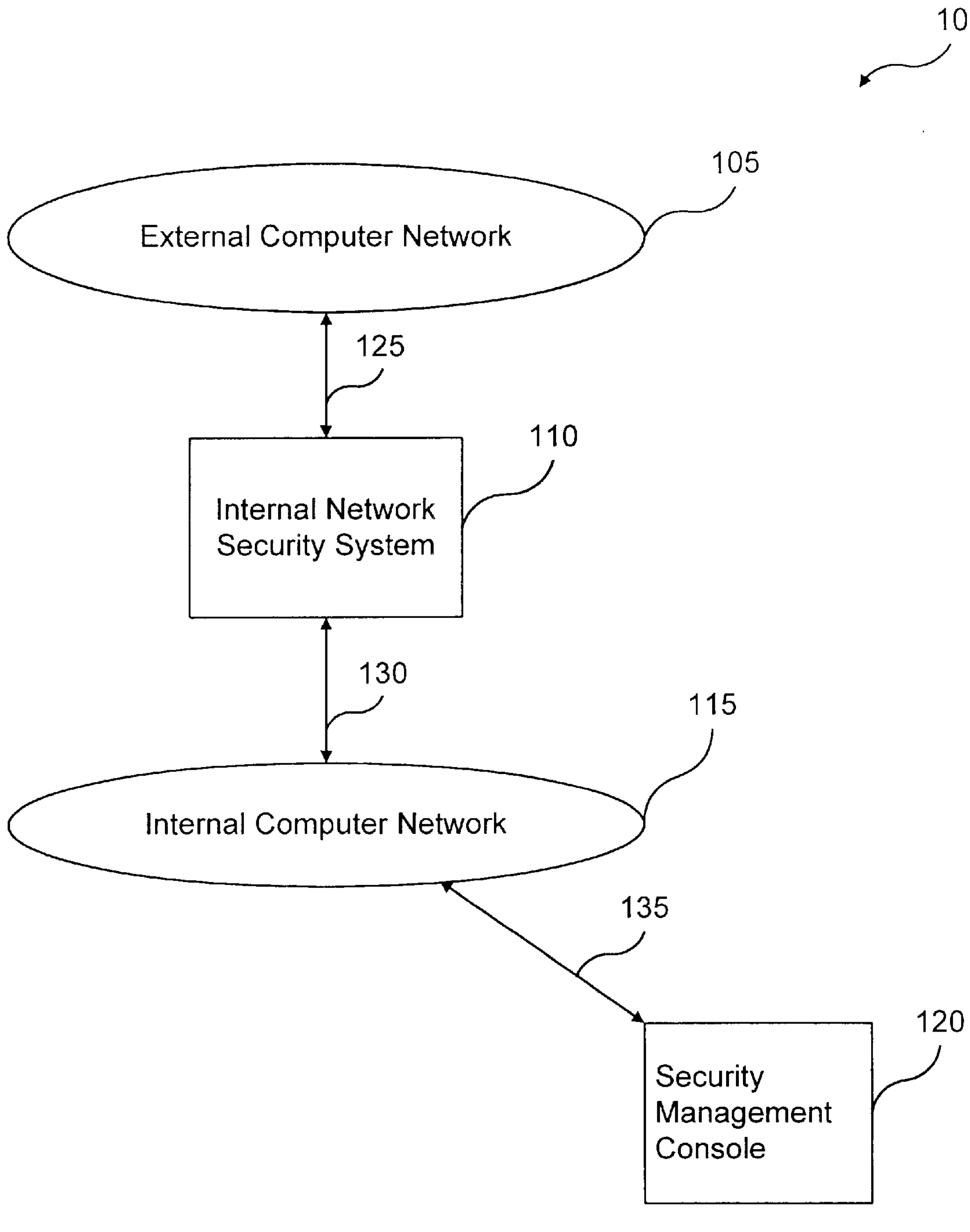

100
105
External Computer Network
125
110
Internal Network Security System
130
115
Internal Computer Network
135
120
Security Management Console

FIG. 1

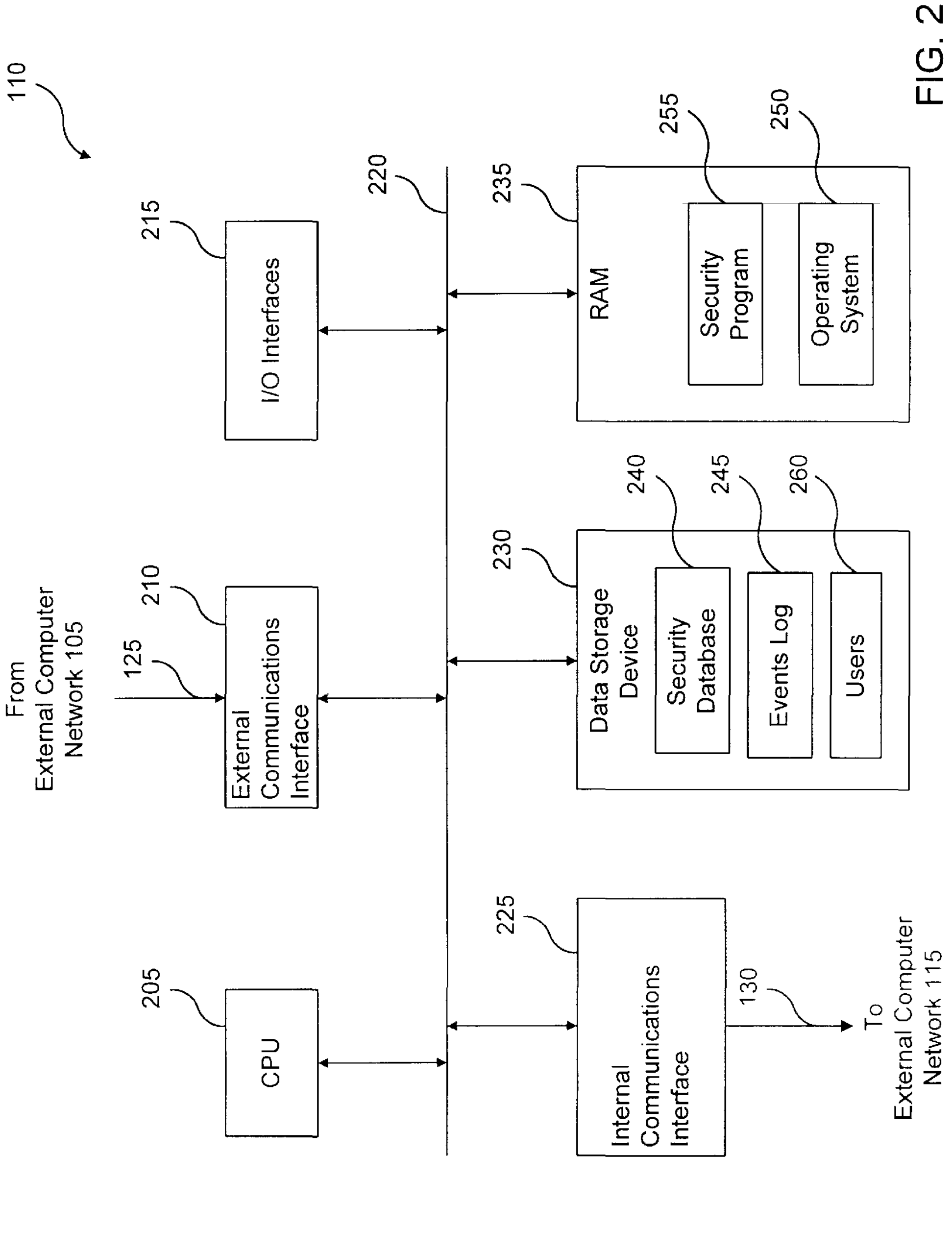

110
215
I/O Interfaces
220
235
RAM
Security Program
Operating System
255
250
210
External Communications Interface
125
From External Computer Network 105
230
Data Storage Device
Security Database
Events Log
Users
240
245
260
205
CPU
225
Internal Communications Interface
130
To External Computer Network 115

FIG. 2

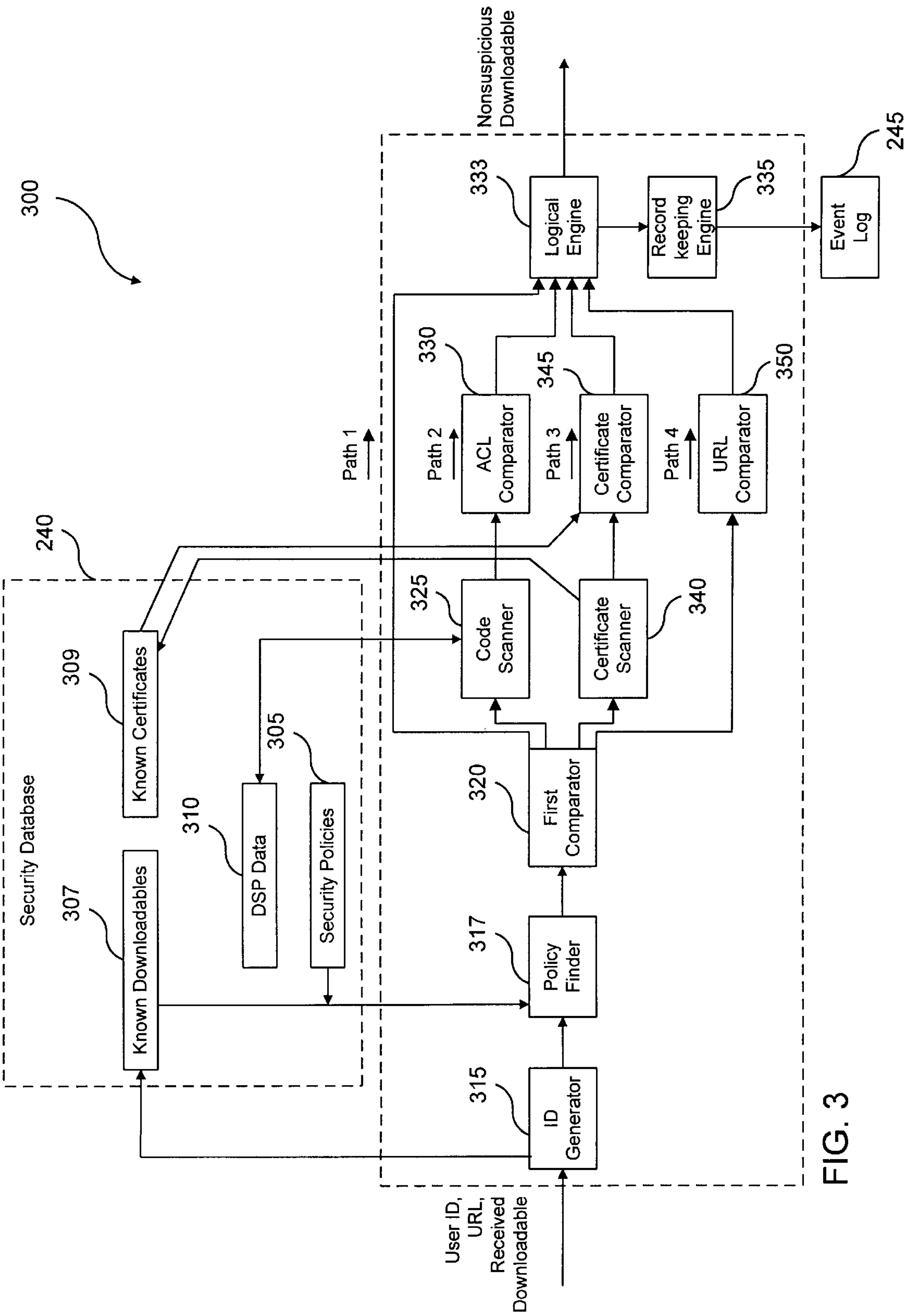

300
240
Security Database
307
Known Downloadables
309
Known Certificates
310
DSP Data
305
Security Policies
User ID,
URL,
Received
Downloadable
315
ID Generator
317
Policy Finder
320
First Comparator
325
Code Scanner
340
Certificate Scanner
Path 1
Path 2
Path 3
Path 4
330
ACL Comparator
345
Certificate Comparator
350
URL Comparator
333
Logical Engine
Nonsuspicious Downloadable
335
Record keeping Engine
245
Event Log

FIG. 3

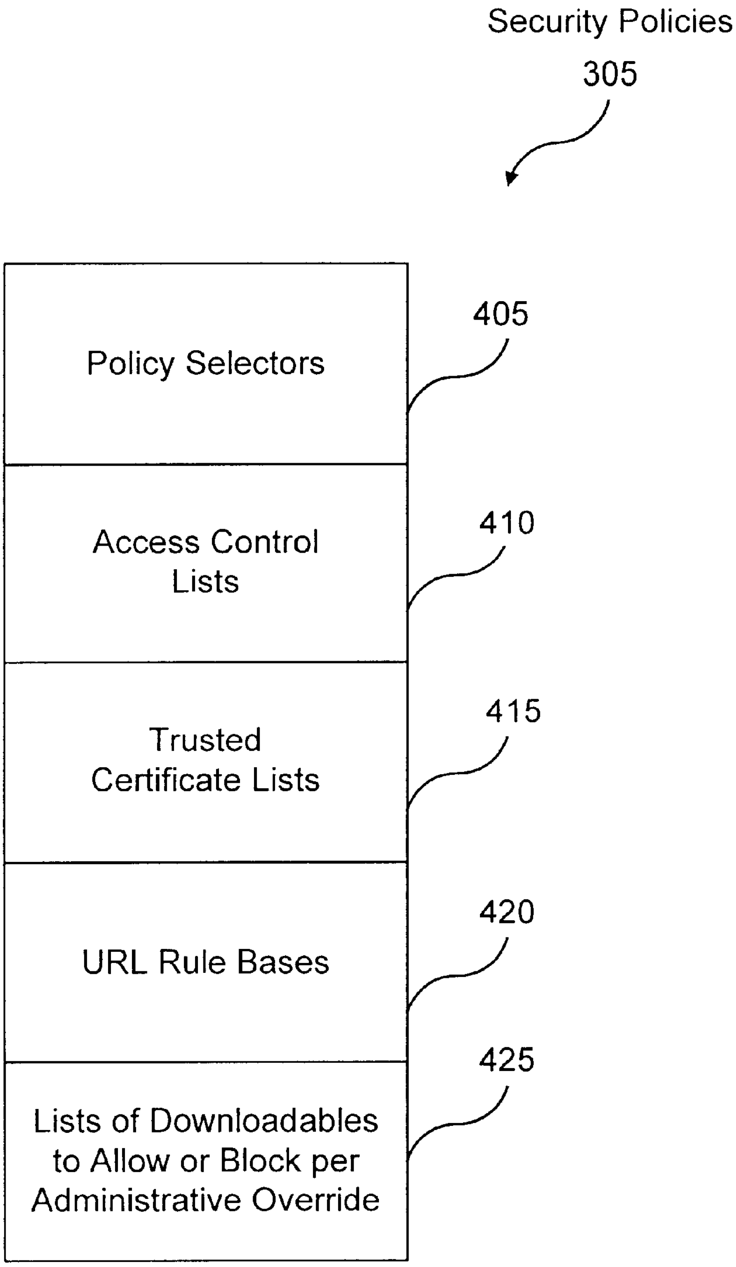

Security Policies
305
Policy Selectors
405
Access Control Lists
410
Trusted Certificate Lists
415
URL Rule Bases
420
Lists of Downloadables to Allow or Block per Administrative Override
425

FIG. 4

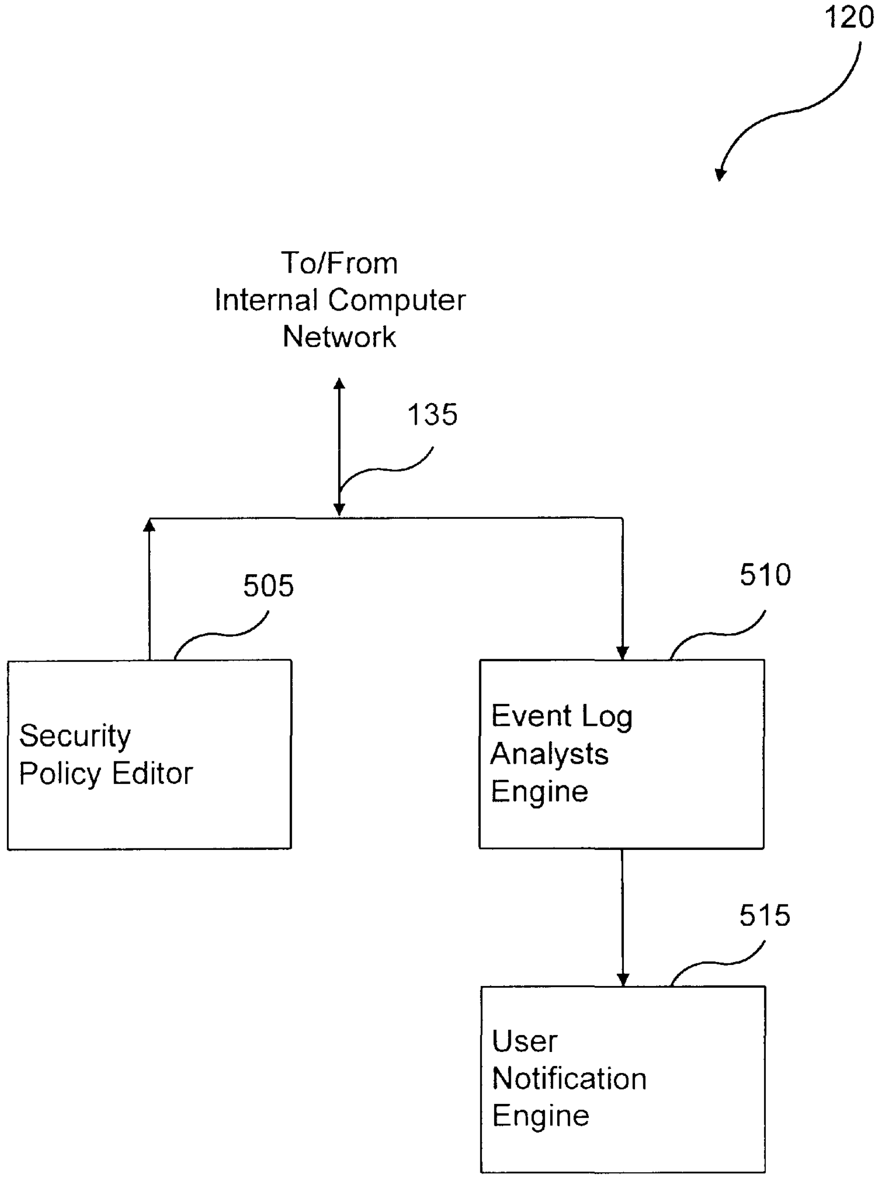

120
To/From
Internal Computer
Network
135
505
510
Security
Policy Editor
Event Log
Analysts
Engine
515
User
Notification
Engine

FIG. 5

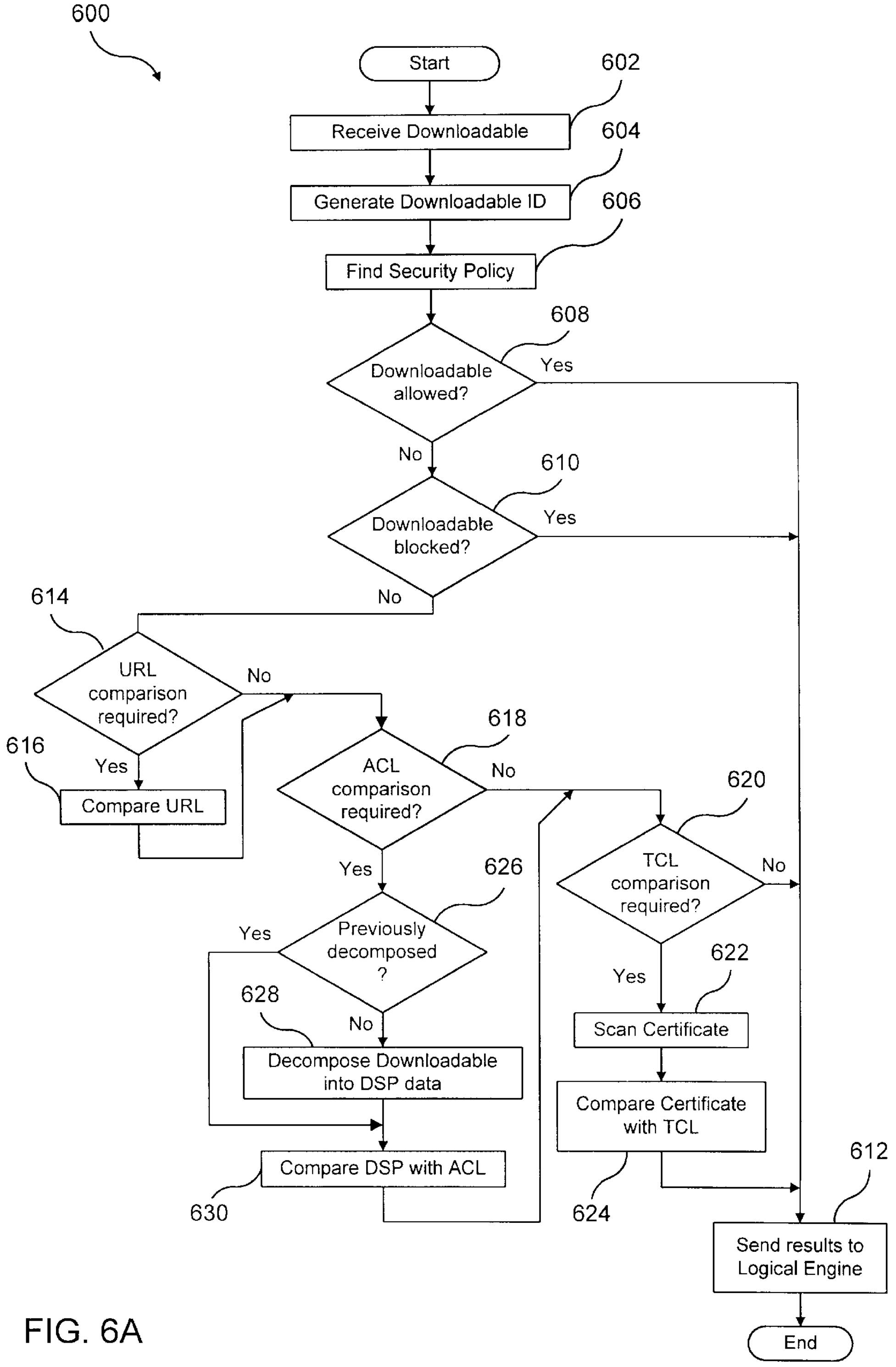

600
Start
602
Receive Downloadable
604
Generate Downloadable ID
606
Find Security Policy
608
Downloadable allowed?
Yes
No
610
Downloadable blocked?
Yes
No
614
URL comparison required?
No
616
Yes
Compare URL
618
ACL comparison required?
No
Yes
626
Previously decomposed ?
Yes
628
No
Decompose Downloadable into DSP data
Compare DSP with ACL
630
620
TCL comparison required?
No
Yes
622
Scan Certificate
Compare Certificate with TCL
624
612
Send results to Logical Engine
End

FIG. 6A

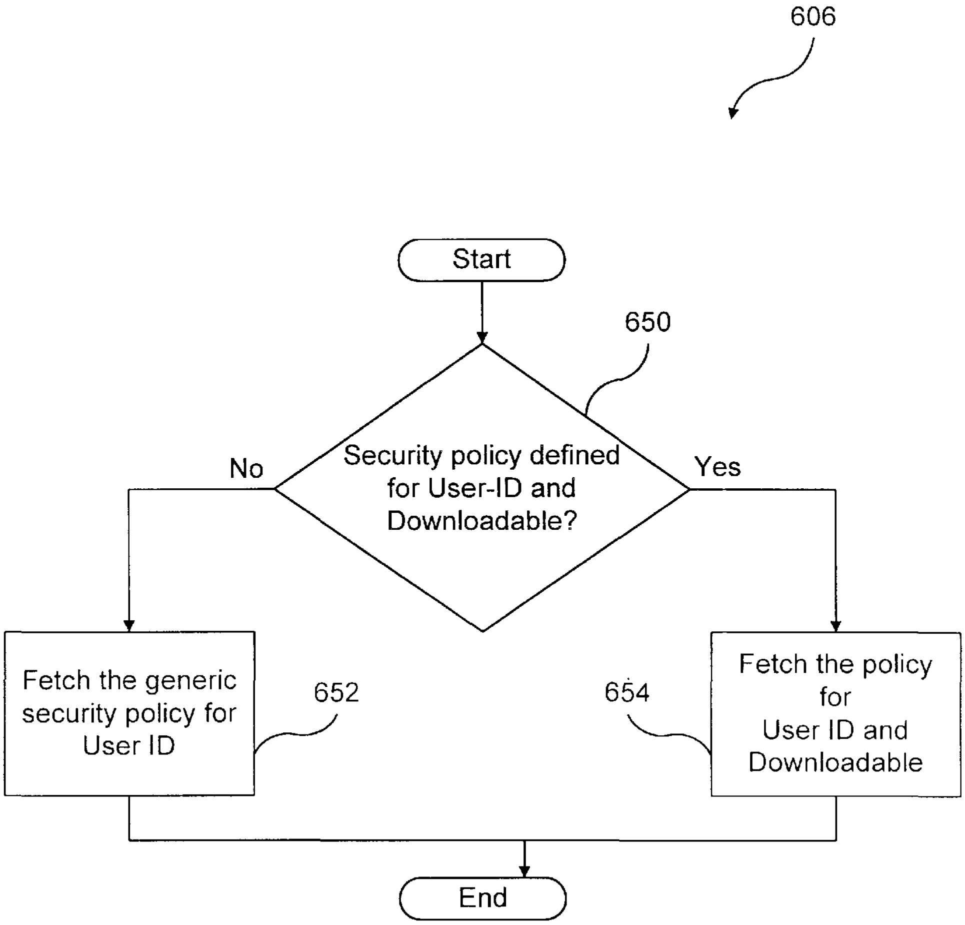

606
Start
650
Security policy defined for User-ID and Downloadable?
No
Yes
Fetch the generic security policy for User ID
652
654
Fetch the policy for User ID and Downloadable
End

FIG. 6B

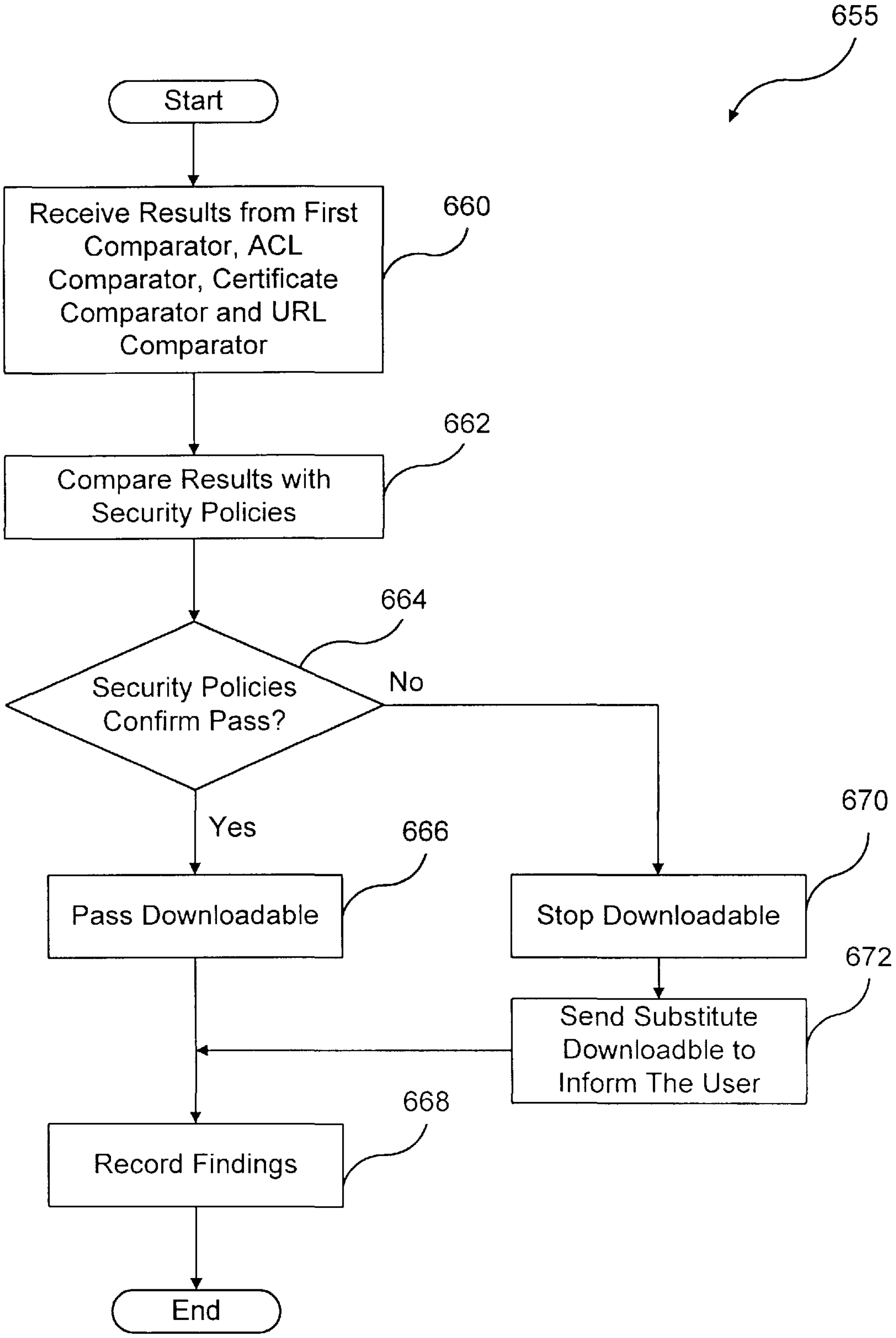

655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
Security Policies Confirm Pass?
664
No
Yes
Pass Downloadable
666
Stop Downloadable
670
Send Substitute Downloadble to Inform The User
672
Record Findings
668
End

FIG. 6C

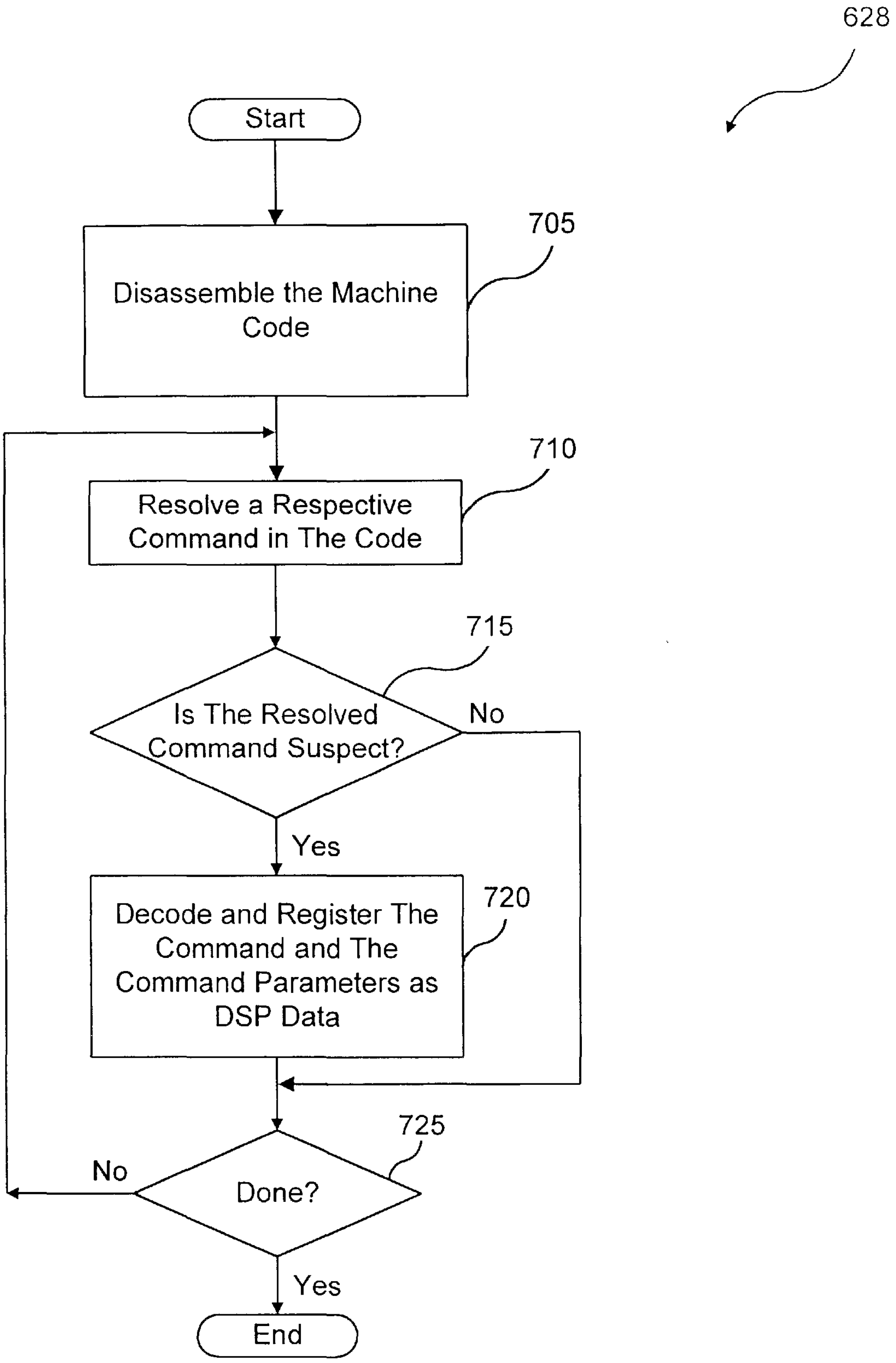

628
Start
Disassemble the Machine Code
705
Resolve a Respective Command in The Code
710
Is The Resolved Command Suspect?
715
No
Yes
Decode and Register The Command and The Command Parameters as DSP Data
720
Done?
725
No
Yes
End

FIG. 7

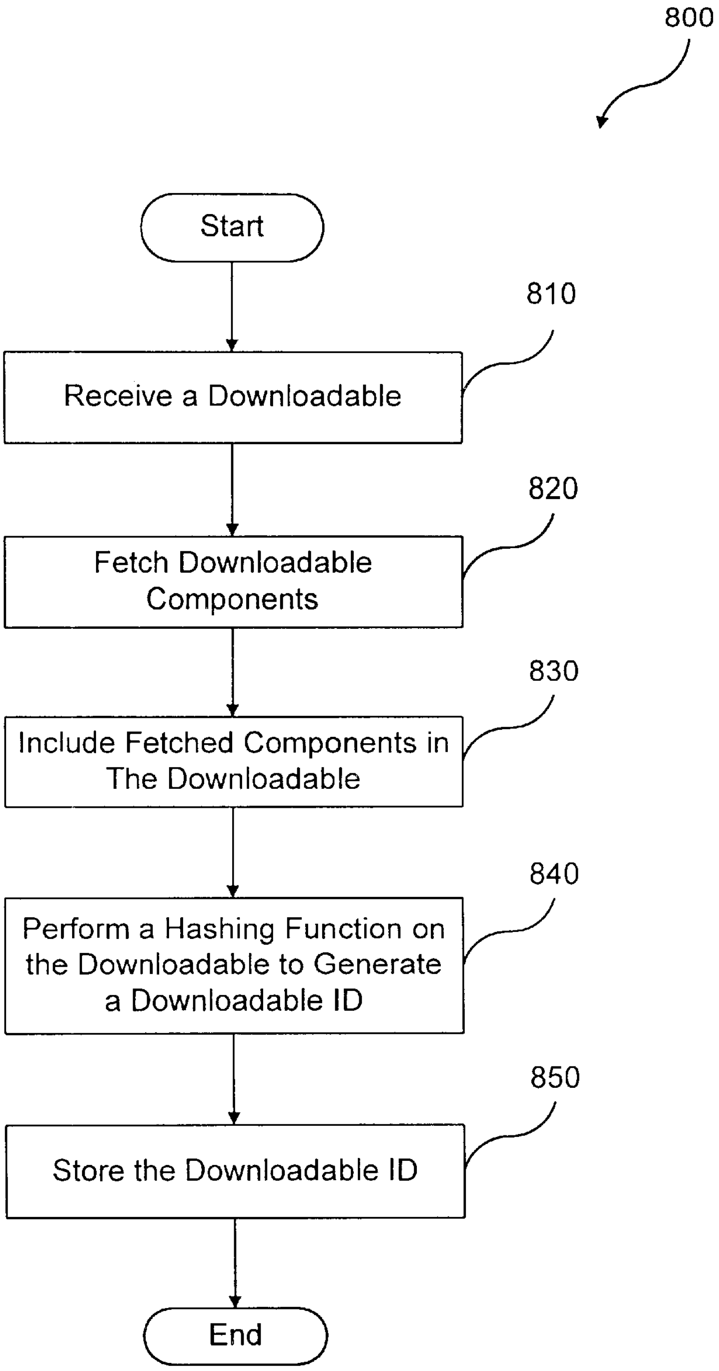

800
Start
810
Receive a Downloadable
820
Fetch Downloadable Components
830
Include Fetched Components in The Downloadable
840
Perform a Hashing Function on the Downloadable to Generate a Downloadable ID
850
Store the Downloadable ID
End

FIG. 8

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

INCORPORATION BY REFERENCE TO RELATED APPLICATION

This application hereby incorporates by reference related U.S. patent application Ser. No. 08/790,097, entitled "System and Method for Protecting a Client from Hostile Downloadables," filed on Jan. 29, 1997, by inventor Shlomo Touboul.

PRIORITY REFERENCE TO PROVISIONAL APPLICATION

This application claims benefit of and hereby incorporates by reference provisional application Ser. No. 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov. 8, 1996, by inventor Shlomo Touboul.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and method for protecting a computer and a network from hostile Downloadables.

2. Description of the Background Art

The Internet is currently a collection of over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate. Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

Accordingly, programmers continue to design computer and computer network security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as "Downloadables." A Downloadable is an executable application program, which is downloaded from a source computer and run on the destination computer. Downloadable is typically requested by an ongoing process such as by an Internet browser or web engine. Examples of Downloadables include Java™ applets designed for use in the Java™ distributing environment developed by Sun Microsystems, Inc., JavaScript scripts also developed by Sun Microsystems, Inc., ActiveX™ controls designed for use in the ActiveX™ distributing environment developed by the Microsoft Corporation, and Visual Basic also developed by the Microsoft Corporation. Therefore, a system and method are needed to protect a network from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a network from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The

security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied based on the client/group and on the particular Downloadable received. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components.

Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

The present invention further provides a method for protecting a computer from suspicious Downloadables. The method comprises the steps of receiving a Downloadable, comparing the Downloadable against a security policy to determine if the security policy has been violated, and discarding the Downloadable if the security policy has been violated.

It will be appreciated that the system and method of the present invention may provide computer protection from known hostile Downloadables. The system and method of the present invention may identify Downloadables that perform operations deemed suspicious. The system and method of the present invention may examine the Downloadable code to determine whether the code contains any suspicious operations, and thus may allow or block the Downloadable accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating a network system, in accordance with the present invention;

FIG. **2** is a block diagram illustrating details of the internal network security system of FIG. **1**;

FIG. **3** is a block diagram illustrating details of the security program and the security database of FIG. **2**;

FIG. **4** is a block diagram illustrating details of the security policies of FIG. **3**;

FIG. **5** is a block diagram illustrating details of the security management console of FIG. **1**;

FIG. **6**A is a flowchart illustrating a method of examining for suspicious Downloadables, in accordance with the present invention;

FIG. **6**B is a flowchart illustrating details of the step for finding the appropriate security policy of FIG. **6**A;

FIG. **6**C is a flowchart illustrating a method for determining whether an incoming Downloadable is to be deemed suspicious;

FIG. **7** is a flowchart illustrating details of the FIG. **6** step of decomposing a Downloadable; and

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a block diagram illustrating a network system **100**, in accordance with the present invention. The network system **100** includes an external computer network **105**, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a communications channel **125** to an internal network security system **110**. The network system **100** further includes an internal computer network **115**, such as a corporate Local Area Network (LAN), coupled via a communications channel **130** to the internal network computer system **110** and coupled via a communications channel **135** to a security management console **120**.

The internal network security system **110** examines Downloadables received from external computer network **105**, and prevents Downloadables deemed suspicious from reaching the internal computer network **115**. It will be further appreciated that a Downloadable is deemed suspicious if it performs or may perform any undesirable operation, or if it threatens or may threaten the integrity of an internal computer network **115** component. It is to be understood that the term "suspicious" includes hostile, potentially hostile, undesirable, potentially undesirable, etc. Security management console **120** enables viewing, modification and configuration of the internal network security system **110**.

FIG. **2** is a block diagram illustrating details of the internal network security system **110**, which includes a Central Processing Unit (CPU) **205**, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a signal bus **220**. The internal network security system **110** further includes an external communications interface **210** coupled between the communications channel **125** and the signal bus **220** for receiving Downloadables from external computer network **105**, and an internal communications interface **225** coupled between the signal bus **220** and the communications channel **130** for forwarding Downloadables not deemed suspicious to the internal computer network **115**. The external communications interface **210** and the internal communications interface **225** may be functional components of an integral communications interface (not shown) for both receiving Downloadables from the external computer network **105** and forwarding Downloadables to the internal computer network **115**.

Internal network security system **110** further includes Input/Output (I/O) interfaces **215** (such as a keyboard, mouse and Cathode Ray Tube (CRT) display), a data storage device **230** such as a magnetic disk, and a Random-Access Memory (RAM) **235**, each coupled to the signal bus **220**. The data storage device **230** stores a security database **240**, which includes security information for determining whether a received Downloadable is to be deemed suspicious. The data storage device **230** further stores a users list **260** identifying the users within the internal computer network **115** who may receive Downloadables, and an event log **245** which includes determination results for each Downloadable examined and runtime indications of the internal network security system **110**. An operating system **250** controls processing by CPU **205**, and is typically stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution. A security program **255** controls examination of incoming Downloadables, and also may be stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution by CPU **205**.

FIG. **3** is a block diagram illustrating details of the security program **255** and the security database **240**. The security program **255** includes an ID generator **315**, a policy finder **317** coupled to the ID generator **315**, and a first comparator **320** coupled to the policy finder **317**. The first comparator **320** is coupled to a logical engine **333** via four separate paths, namely, via Path 1, via Path 2, via Path 3 and via Path 4. Path 1 includes a direct connection from the first comparator **320** to the logical engine **333**. Path 2 includes a code scanner coupled to the first comparator **320**, and an Access Control List (ACL) comparator **330** coupling the code scanner **325** to the logical engine **333**. Path 3 includes a certificate scanner **340** coupled to the first comparator **320**, and a certificate comparator **345** coupling the certificate scanner **340** to the logical engine **333**. Path 4 includes a Uniform Resource Locator (URL) comparator **350** coupling the first comparator **320** to the logical engine **3330**. A record-keeping engine **335** is coupled between the logical engine **333** and the event log **245**.

The security program **255** operates in conjunction with the security database **240**, which includes security policies **305**, known Downloadables **307**, known Certificates **309** and Downloadable Security Profile (DSP) data **310** corresponding to the known Downloadables **307**. Security policies **305** includes policies specific to particular users **260** and default (or generic) policies for determining whether to allow or block an incoming Downloadable. These security policies **305** may identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable. Referring to FIG. **4**, security policies **305** include policy selectors **405**, access control lists **410**, trusted certificate lists **415**, URL rule bases **420**, and lists **425** of Downloadables to allow or to block per administrative override.

Known Downloadables **307** include lists of Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, of Downloadables which OEMs know to be non-hostile, and of Downloadables previously received by this security program **255**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by each known Downloadable **307**, and may also include the respective arguments of these operations. An identified argument of an operation is referred to as "resolved." An unidentified argument is referred to as "unresolved." DSP data **310** is described below with reference to the code scanner **325**.

The ID generator **315** receives a Downloadable (including the URL from which it came and the userID of the intended recipient) from the external computer network **105** via the external communications interface **210**, and generates a Downloadable ID for identifying each Downloadable. The Downloadable ID preferably includes a digital hash of the complete Downloadable code. The ID generator **315** preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator **315** may prefetch all classes embodied in or identified by the Java™ applet bytecode to generate the Downloadable ID. Similarly, the ID generator **315** may retrieve all components listed in the .INF file for an ActiveX™ control to compute a Downloadable ID. Accordingly, the Downloadable ID for the Downloadable will be the same each time the ID generator **315** receives the same Downloadable. The ID generator **315** adds the generated Downloadable ID to the list of known Downloadables **307** (if it is not already listed). The ID generator **315** then forwards the Downloadable and Downloadable ID to the policy finder **317**.

The policy finder **317** uses the userID of the intended user and the Downloadable ID to select the specific security policy **305** that shall be applied on the received Downloadable. If there is a specific policy **305** that was defined for the user (or for one of its super groups) and the Downloadable, then the policy is selected. Otherwise the generic policy **305** that was defined for the user (or for one of its super groups) is selected. The policy finder **317** then sends the policy to the first comparator **320**.

The first comparator **320** receives the Downloadable, the Downloadable ID and the security policy **305** from the policy finder **317**. The first comparator **320** examines the security policy **305** to determine which steps are needed for allowing the Downloadable. For example, the security policy **305** may indicate that, in order to allow this Downloadable, it must pass all four paths, Path 1, Path 2, Path 3 and Path 4. Alternatively, the security policy **305** may indicate that to allow the Downloadable, it must pass only one of the paths. The first comparator **320** responds by forwarding the proper information to the paths identified by the security policy **305**.

Path 1

In path 1, the first comparator **320** checks the policy selector **405** of the security policy **305** that was received from the policy finder **317**. If the policy selector **405** is either "Allowed" or "Blocked," then the first comparator **320** forwards this result directly to the logical engine **333**. Otherwise, the first comparator **320** invokes the comparisons in path 2 and/or path 3 and/or path 4 based on the contents of policy selector **405**. It will be appreciated that the first comparator **320** itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override **425**. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked."

Alternatively, the logical engine **333** may receive the results of each of the paths and based on the policy selector **405** may institute the final determination whether to allow or block the Downloadable. The first comparator **320** informs the logical engine **333** of the results of its comparison.

Path 2

In path 2, the first comparator **320** delivers the Downloadable, the Downloadable ID and the security policy **305** to the code scanner **325**. If the DSP data **310** of the received Downloadable is known, the code scanner **325** retrieves and forwards the information to the ACL comparator **330**. Otherwise, the code scanner **325** resolves the DSP data **310**. That is, the code scanner **325** uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data **310**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable **307**, and may also include the respective arguments of these operations. For example, DSP data **310** may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner **325** may generate the DSP data **310** as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner **325** may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker.

An Example List of Operations Deemed Potentially Hostile

File operations: READ a file, WRITE a file;

Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET;

Registry operations: READ a registry item, WRITE a registry item;

Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAD, KILL PROCESS/THREAD, CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc.; and

Resource usage thresholds: memory, CPU, graphics, etc.

In the preferred embodiment, the code scanner **325** performs a full-content inspection. However, for improved speed but reduced security, the code scanner **325** may examine only a portion of the Downloadable such as the Downloadable header. The code scanner **325** then stores the DSP data into DSP data **310** (corresponding to its Downloadable ID), and sends the Downloadable, the DSP data to the ACL comparator **330** for comparison with the security policy **305**.

The ACL comparator **330** receives the Downloadable, the corresponding DSP data and the security policy **305** from the code scanner **325**, and compares the DSP data against the security policy **305**. That is, the ACL comparator **330** compares the DSP data of the received Downloadable against the access control lists **410** in the received security policy **305**. The access control list **410** contains criteria indicating whether to pass or fail the Downloadable. For example, an access control list may indicate that the Downloadable fails if the DSP data includes a WRITE command to a system file. The ACL comparator **330** sends its results to the logical engine **333**.

Path 3

In path 3, the certificate scanner **340** determines whether the received Downloadable was signed by a certificate authority, such as VeriSign, Inc., and scans for a certificate embodied in the Downloadable. The certificate scanner **340** forwards the found certificate to the certificate comparator **345**. The certificate comparator **345** retrieves known certificates **309** that were deemed trustworthy by the security administrator and compares the found certificate with the known certificates **309** to determine whether the Downloadable was signed by a trusted certificate. The certificate comparator **345** sends the results to the logical engine **333**.

Path 4

In path 4, the URL comparator **350** examines the URL identifying the source of the Downloadable against URLs stored in the URL rule base **420** to determine whether the Downloadable comes from a trusted source. Based on the security policy **305**, the URL comparator **350** may deem the Downloadable suspicious if the Downloadable comes from an untrustworthy source or if the Downloadable did not come from a trusted source. For example, if the Downloadable comes from a known hacker, then the Downloadable may be deemed suspicious and presumed hostile. The URL comparator **350** sends its results to the logical engine **333**.

The logical engine **333** examines the results of each of the paths and the policy selector **405** in the security policy **305** to determine whether to allow or block the Downloadable. The policy selector **405** includes a logical expression of the results received from each of the paths. For example, the logical engine **333** may block a Downloadable if it fails any one of the paths, i.e., if the Downloadable is known hostile (Path 1), if the Downloadable may request suspicious operations (Path 2), if the Downloadable was not signed by a trusted certificate authority (Path 3), or if the Downloadable came from an untrustworthy source (Path 4). The logical engine **333** may apply other logical expressions according to the policy selector **405** embodied in the security policy **305**. If the policy selector **405** indicates that the Downloadable may pass, then the logical engine **333** passes the Downloadable to its intended recipient. Otherwise, if the policy selector **405** indicates that the Downloadable should be blocked, then the logical engine **333** forwards a non-hostile Downloadable to the intended recipient to inform the user that internal network security system **110** discarded the original Downloadable. Further, the logical engine **333** forwards a status report to the record-keeping engine **335**, which stores the reports in event log **245** in the data storage device **230** for subsequent review, for example, by the MIS director.

FIG. **5** is a block diagram illustrating details of the security management console **120**, which includes a security policy editor **505** coupled to the communications channel **135**, an event log analysis engine **510** coupled between communications channel **135** and a user notification engine **515**, and a Downloadable database review engine **520** coupled to the communications channel **135**. The security management console **120** further includes computer components similar to the computer components illustrated in FIG. **2**.

The security policy editor **505** uses an I/O interface similar to I/O interface **215** for enabling authorized user modification of the security policies **305**. That is, the security policy editor **505** enables the authorized user to modify specific security policies **305** corresponding to the users **260**, the default or generic security policy **305**, the Downloadables to block per administrative override, the Downloadables to allow per administrative override, the trusted certificate lists **415**, the policy selectors **405**, the access control lists **410**, the URLs in the URL rule bases **420**, etc. For example, if the authorized user learns of a new hostile Downloadable, then the user can add the Downloadable to the Downloadables to block per system override.

The event log analysis engine **510** examines the status reports contained in the event log **245** stored in the data storage device **230**. The event log analysis engine **510** determines whether notification of the user (e.g., the security system manager or MIS director) is warranted. For example, the event log analysis engine **510** may warrant user notification whenever ten (10) suspicious Downloadables have been discarded by internal network security system **110** within a thirty (30) minute period, thereby flagging a potential imminent security threat. Accordingly, the event log analysis engine **510** instructs the user notification engine **515** to inform the user. The user notification engine **515** may send an e-mail via internal communications interface **220** or via external communications interface **210** to the user, or may display a message on the user's display device (not shown).

FIG. **6**A is a flowchart illustrating a method **600** for protecting an internal computer network **115** from suspicious Downloadables. Method **600** begins with the ID generator **315** in step **602** receiving a Downloadable. The ID generator **315** in step **604** generates a Downloadable ID identifying the received Downloadable, preferably, by generating a digital hash of the Downloadable code (including prefetched components). The policy finder **317** in step **606** finds the appropriate security policy **305** corresponding to the userID specifying intended recipient (or the group to which the intended recipient belongs) and the Downloadable. The selected security policy **305** may be the default security policy **305**. Step **606** is described in greater detail below with reference to FIG. **6**B.

The first comparator **320** in step **608** examines the lists of Downloadables to allow or to block per administrative override **425** against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically. If so, then in step **612** the first comparator **320** sends the results to the logical engine **333**. If not, then the method **600** proceeds to step **610**. In step **610**, the first comparator **620** examines the lists of Downloadables to block per administrative override **425** against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically. If so, then the first comparator **420** in step **612** sends the results to the logical engine **333**. Otherwise, method **600** proceeds to step **614**.

In step **614**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 4. If not, then method **600** jumps to step **618**. If so, then the URL comparator **350** in step **616** compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases **420**, and then method **600** proceeds to step **618**.

In step **618**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 2. If not, then method **600** jumps to step **620**. Otherwise, the code scanner **235** in step **626** examines the DSP data **310** based on the Downloadable ID of the incoming Downloadable to determine whether the Downloadable has been previously decomposed. If so, then method **600** jumps to step **630**. Otherwise, the code scanner **325** in step **628** decomposes the Downloadable into DSP data. Downloadable decomposition is described in greater detail with reference to FIG. **7**. In step **630**, the ACL comparator **330** compares the DSP data of the incoming Downloadable against the access control lists **410** (which include the criteria necessary for the Downloadable to fail or pass the test).

In step **620**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path 3. If not, then method **600** returns to step **612** to send the results of each of the test performed to the logical engine **333**. Otherwise, the certificate scanner **622** in step **622** scans the Downloadable for an embodied certificate. The certificate comparator **345** in step **624** retrieves trusted certificates from the trusted certificate lists (TCL) **415** and compares the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source. Method **600** then proceeds to step **612** by the certificate scanner **345** sending the results of each of the paths taken to the logical engine **333**. The operations of the logical engine **333** are described in greater detail below with reference to FIG. **6**C. Method **600** then ends.

One skilled in the art will recognize that the tests may be performed in a different order, and that each of the tests need not be performed. Further, one skilled in the art will recognize that, although path 1 is described in FIG. **6**A as an automatic allowance or blocking, the results of Path 1 may be another predicate to be applied by the logical engine **333**. Further, although the tests are shown serially in FIG. **6**A, the tests may be performed in parallel as illustrated in FIG. **3**.

FIG. **6**B is a flowchart illustrating details of step **606** of FIG. **6**A (referred to herein as method **606**). Method **606** begins with the policy finder **317** in step **650** determining whether security policies **305** include a specific security policy corresponding to the userID and the Downloadable. If so, then the policy finder **317** in step **654** fetches the corresponding specific policy **305**. If not, then the policy finder **317** in step **652** fetches the default or generic security policy **305** corresponding to the userID. Method **606** then ends.

FIG. **6**C is a flowchart illustrating details of a method **655** for determining whether to allow or to block the incoming Downloadable. Method **655** begins with the logical engine **333** in step **660** receiving the results from the first comparator **320**, from the ACL comparator **330**, from the certificate comparator **345** and from the URL comparator **350**. The logical engine **333** in step **662** compares the results with the policy selector **405** embodied in the security policy **305**, and in step **664** determines whether the policy selector **405** confirms the pass. For example, the policy selector **405** may indicate that the logical engine **333** pass the Downloadable if it passes one of the tests of Path 1, Path 2, Path 3 and Path 4. If the policy selector **405** indicates that the Downloadable should pass, then the logical engine **333** in step **666** passes the Downloadable to the intended recipient. In step **668**, the logical engine **333** sends the results to the record-keeping engine **335**, which in turn stores the results in the event log **245** for future review. Method **655** then ends. Otherwise, if the policy selector **405** in step **664** indicates that the Downloadable should not pass, then the logical engine **333** in step **670** stops the Downloadable and in step **672** sends a non-hostile substitute Downloadable to inform the user that the incoming Downloadable has been blocked. Method **655** then jumps to step **668**.

FIG. **7** is a flowchart illustrating details of step **628** of FIG. **6**A (referred to herein as method **628**) for decomposing a Downloadable into DSP data **310**. Method **628** begins in step **705** with the code scanner **325** disassembling the machine code of the Downloadable. The code scanner **325** in step **710** resolves a respective command in the machine code, and in step **715** determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. **3**). If not, then the code scanner **325** in step **725** determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method **628** ends. Otherwise, method **628** returns to step **710**.

Otherwise, if the code scanner **325** in step **715** determines that the resolved command is suspect, then the code scanner **325** in step **720** decodes and registers the suspicious command and its command parameters as DSP data **310**. The code scanner **325** in step **720** registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method **628** then jumps to step **725**.

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable. Method **800** begins with the ID generator **315** in step **810** receiving a Downloadable from the external computer network **105**. The ID generator **315** in step **820** may fetch some or all components referenced in the Downloadable code, and in step **830** includes the fetched components in the Downloadable code. The ID generator **315** in step **840** performs a hashing function on at least a portion of the Downloadable code to generate a Downloadable ID. The ID generator **315** in step **850** stores the generated Downloadable ID in the security database **240** as a reference to the DSP data **310**. Accordingly, the Downloadable ID will be the same for the identical Downloadable each time it is encountered.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method, comprising the steps of:

receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client;

comparing, by the server, Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and

preventing execution of the Downloadable by the client if the security policy has been violated.

2. The method of claim **1**, further comprising the step of decomposing the Downloadable into the Downloadable security profile data.

3. The method of claim **2**, wherein the security policy includes an access control list and further comprising the step of comparing the Downloadable security profile data against the access control list.

4. The method of claim **1**, further comprising the steps of scanning for a certificate and comparing the certificate against a trusted certificate.

5. The method of claim **1**, further comprising the step of comparing the URL from which the Downloadable originated against a known URL.

6. The method of claim **5**, wherein the known URL is a trusted URL.

7. The method of claim **5**, wherein the known URL is an untrusted URL.

8. The method of claim **1**, wherein the Downloadable includes a Java™ applet.

9. The method of claim **1**, wherein the Downloadable includes an ActiveX™ control.

10. The method of claim **1**, wherein the Downloadable includes a JavaScript™ script.

11. The method of claim **1**, wherein the Downloadable includes a Visual Basic script.

12. The method of claim **1**, wherein

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

13. The method of claim **1**, wherein

the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

14. The method of claim **1**, wherein

the client belongs to a particular group; and

the security policy includes a specific security policy corresponding to the particular group.

15. The method of claim **1**, further comprising, after preventing execution of the Downloadable, the step of sending a substitute non-hostile Downloadable to the client for informing the client.

16. The method of claim **1**, further comprising, after preventing execution of the Downloadable, the step of recording the violation in an event log.

17. The method of claim **1**, further comprising the step of computing a Downloadable ID to identify the Downloadable.

18. The method of claim **16**, further comprising the steps of fetching components identified by the Downloadable and including the fetched components in the Downloadable.

19. The method of claim **18**, further comprising the step of performing a hashing function on the Downloadable to compute a Downloadable ID to identify the Downloadable.

20. The method of claim **18**, further comprising the step of fetching all components identified by the Downloadable.

21. The method of claim **1** further comprising the step of examining the intended recipient userID to determine the appropriate security policy.

22. The method of claim **20**, wherein the appropriate security policy includes a default security policy.

23. The method of claim **1**, further comprising the step of examining the Downloadable to determine the appropriate security policy.

24. The method of claim **1**, further comprising the step of comparing the Downloadable against a known Downloadable.

25. The method of claim **24**, wherein the known Downloadable is hostile.

26. The method of claim **24**, wherein the known Downloadable is non-hostile.

27. The method of claim **24**, further comprising the step of including a previously received Downloadable as a known Downloadable.

28. The method of claim **27**, wherein the security policy identifies a Downloadable to be blocked per administrative override.

29. The method of claim **28**, wherein the security policy identifies a Downloadable to be allowed per administrative override.

30. The method of claim **1**, further comprising the step of informing a user upon detection of a security policy violation.

31. The method of claim **1**, further comprising the steps of recognizing the incoming Downloadable, and obtaining the Downloadable security profile data for the incoming Downloadable from memory.

32. A system for execution by a server that serves as a gateway to a client, the system comprising:

a security policy;

an interface for receiving an incoming Downloadable addressed to a client;

a comparator, coupled to the interface, for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against the security policy to determine if the security policy has been violated; and

a logical engine for preventing execution of the Downloadable by the client if the security policy has been violated.

33. The system of claim **32**, wherein the Downloadable includes a Java™ applet.

34. The system of claim **32**, wherein the Downloadable includes ActiveX™ control.

35. The system of claim **32**, wherein the Downloadable includes a JavaScript™ script.

36. The system of claim **32**, wherein the Downloadable includes a Visual Basic script.

37. The system of claim **32**, wherein

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

38. The system of claim **32**, wherein

the security policy includes a specific security policy corresponding to the client to whom the Downloadable is addressed.

39. The system of claim **32**, wherein

the client belongs to a particular group; and

the security policy includes a specific security policy corresponding to the particular group.

40. The system of claim **32**, further comprising an ID generator coupled to the interface for computing a Downloadable ID identifying the Downloadable.

41. The system of claim **40**, wherein the ID generator prefetches all components of the Downloadable and uses all components to compute the Downloadable ID.

42. The system of claim **41**, wherein the ID generator computes the digital hash of all the prefetched components.

43. The system of claim **32**, further comprising a policy finder for finding the security policy.

44. The system of claim **43**, wherein the policy finder finds the security policy based on the user.

45. The system of claim **43** wherein the policy finder finds the security policy based on the user and the Downloadable.

46. The system of claim **43**, wherein the policy finder obtains the default security policy.

47. The system of claim **32** wherein the comparator examines the security policy to determine which tests to apply.

48. The system of claim **47** wherein the comparator compares the Downloadable against a known Downloadable.

49. The system of claim **48**, wherein the known Downloadable is hostile.

50. The system of claim **48**, wherein the known Downloadable is non-hostile.

51. The system of claim **32**, wherein the security policy identifies a Downloadable to be blocked per administrative override.

52. The system of claim **32**, wherein the security policy identifies a Downloadable to be allowed per administrative override.

53. The system of claim **32**, wherein

the comparator sends a substitute non-hostile Downloadable to the client for informing the client.

54. The system of claim **32**, further comprising a code scanner coupled to the comparator for decomposing the Downloadable into the Downloadable security profile data.

55. The system of claim **54**, further comprising an ACL comparator coupled to the code scanner for comparing the Downloadable security profile data against an access control list.

56. The system of claim **32**, further comprising a certificate scanner coupled to the comparator for examining the Downloadable for a certificate.

57. The system of claim **56**, further comprising a certificate comparator coupled to the certificate scanner for comparing the certificate against a trusted certificate.

58. The system of claim **32**, further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL.

59. The system of claim **58**, wherein the known URL identifies an untrusted URL.

60. The system of claim **58**, wherein the known URL identifies a trusted URL.

61. The system of claim **31**, wherein the logical engine responds according to the security policy.

62. The system of claim **31**, further comprising a recordkeeping engine coupled to the comparator for recording results in an event log.

63. The system of claim **32**, further comprising memory storing the Downloadable security profile data for the incoming Downloadable.

64. A system for execution on a server that serves as a gateway to a client, comprising:

means for receiving an incoming Downloadable addressed to a client;

means for comparing Downloadable security profile data pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, against a security policy to determine if the security policy has been violated; and

means for preventing execution of the Downloadable by the client if the security policy has been violated.

65. A computer-readable storage medium storing program code for causing a server that serves as a gateway to a client to perform the steps of:

receiving an incoming Downloadable addressed to a client;

comparing Downloadable security profile data pertaining to the Downloadable against a security policy to determine if the security policy has been violated; and

preventing execution of the Downloadable by the client if the security policy has been violated.

66. A method, comprising:

receiving a Downloadable;

decomposing the Downloadable into Downloadable security profile data; the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable,

comparing the Downloadable security profile data against a security policy; and

preventing execution of the Downloadable if the Downloadable security profile data violates the security policy.

67. The method of claim **66**, further comprising:

fetching all components referenced by the Downloadable;

performing a hashing function of the Downloadable and the components fetched to compute a Downloadable ID; and

storing the Downloadable security profile data and the Downloadable ID in memory.

68. A method, comprising:

providing memory storing known-Downloadable security profile data and a that includes a list a suspicious computer operations that may be attempted by a Downloadable known-Downloadable ID corresponding to the Downloadable security profile data;

receiving an incoming Downloadable;

fetching all components referenced by the incoming Downloadable;

performing a hashing function of the Downloadable and the components to compute an incoming-Downloadable ID;

comparing the known-Downloadable ID against the incoming-Downloadable ID;

retrieving the Downloadable security profile data if the known-Downloadable ID and the incoming-Downloadable ID match; and

comparing the Downloadable security profile data against a security policy to determine if the incoming Downloadable violates the security policy.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,092,194 Page 1 of 1
DATED : July 18, 2000
INVENTOR(S) : Shlomo Touboul

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 13,
Line 19, after "to the Downloadable" and before "against a security" insert --, the Downloadable security profile data includes a list a suspicious computer operations that may be attempted by the Downloadable, --

Column 14,
Line 12, after "profile data and" and before "that includes" delete -- a --

Signed and Sealed this

Fifth Day of February, 2002

Attest:

JAMES E. ROGAN

Attesting Officer

Director of the United States Patent and Trademark Office

US006092194C1

(12) EX PARTE REEXAMINATION CERTIFICATE (7004th)

United States Patent (10) **Number: US 6,092,194 C1**

Touboul (45) **Certificate Issued: Aug. 18, 2009**

(54) **SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND NETWORK FROM HOSTILE DOWNLOADABLES**

(75) Inventor: **Shlomo Touboul**, Kefar-Haim (IL)

(73) Assignee: **Finjan Software, Ltd.**, Netanya (IL)

Reexamination Request:
No. 90/009,175, Jun. 6, 2008

Reexamination Certificate for:

Patent No.:	**6,092,194**
Issued:	**Jul. 18, 2000**
Appl. No.:	**08/964,388**
Filed:	**Nov. 6, 1997**

Certificate of Correction issued Feb. 5, 2002.

Related U.S. Application Data

(60) Provisional application No. 60/030,639, filed on Nov. 8, 1996.

(51) **Int. Cl.**

G06F 1/00	(2006.01)
G06F 21/00	(2006.01)

(52) **U.S. Cl.** **726/24**

(58) **Field of Classification Search** .... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,359,659	A	10/1994	Rosenthal	726/24
5,398,196	A	3/1995	Chambers	
5,412,717	A	5/1995	Fischer	713/156
5,414,833	A	5/1995	Hershey et al.	395/575
5,692,047	A	11/1997	McManis	
5,740,441	A	4/1998	Yellin et al.	395/704
5,825,877	A	10/1998	Dan	
5,859,966	A	1/1999	Hayman et al.	726/23
5,864,683	A	1/1999	Boebert et al.	
5,951,698	A	9/1999	Chen et al.	714/38
5,956,481	A	9/1999	Walsh et al.	726/23
5,974,549	A	10/1999	Golan	726/23
5,983,348	A	11/1999	Ji	726/13
6,263,442	B1	7/2001	Mueller et al.	713/201
6,571,338	B1	5/2003	Shaio et al.	713/201

FOREIGN PATENT DOCUMENTS

JP	08-263447	10/1996

OTHER PUBLICATIONS

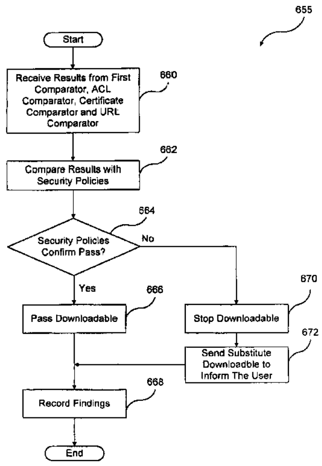
"WWW Proxy to cut off Java," message from Carl Claunch dated Apr. 12, 1996 available at http://groups.google.com/group/muc.lists.firewalls/msg/38bb246b7eb3bec3.

(Continued)

Primary Examiner—Christopher E Lee

(57) **ABSTRACT**

A system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.


655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
Security Policies Confirm Pass?
664
No
Yes
Pass Downloadable
666
Stop Downloadable
670
Send Substitute Downloadble to Inform The User
672
Record Findings
668
End

OTHER PUBLlCATlONS

"lmproved JavaScript and Java screening function," message from Carl Claunch dated May 4, 1996, available at http://groups.google.com/group/muc.lists.firewalls/msg/96bc8043476ab0b7.

"New version of Java, JavaScript, ActiveX screening http–gw patch," message from Carl Claunch dated Jul. 3, 1996 available at http://groups.google.com/group/muc.lists.firewalls/msg/41a45c2a9d5373f2.

"Java Blocking," message from Carl Claunch dated Sep. 25, 1996 available at http://groups.google.com/group/muc.lists.firewalls/msg/2a5ec02e00a37071.

F. M. Avolio and M. J. Ranum, "A Toolkit and Methods for lnternet Firewalls," ln Technical Summer Conference, pp. 37–44, Boston, Massachusetts, Jun. 1994, USENlX. available at http://citeseer.ist.psu.edu.ranum94toolkit.html.

M. M. King, "ldentifying and Controlling Undesirable Program Behaviors," Proceedings of the 14th National Computer Security Conference, 1991.

D. Wichers, D. Cook, R. Olsson, J. Crossley, P. Kerchen, K. Levitt, and R. Lo. "PACL's: an access control list approach to anti–viral security". ln USENlX Workshop Proceedings. UNlX Security ll, pp. 71–82, 1990.

Janet Endrijonas, "Rx PC, the Anti–Virus Handbook," 1–9 (McGraw Hill 1993).

lnternational Search Report for Application No. PCT/lB97/01626, dated May 14, 2999, 2 pp.

Zhang, X. N., "Secure Code Distribution," *Computer*, vol. 30, pp. 76–79, Jun. 1997.

"lBM AntiVirus User's Guide Version 2.4," lnternational Business Machines Corporation, pp. 6–7, Nov. 15, 1995.

Supplementary European Search Report for Application No. EP 97 95 0351, dated Nov. 17, 2004, 2 pp.

"Part 2: Java Vs. VBS—Breadth of Runtime Environments and Security Make Java a Good Choice for the lnternet," Nikkei Electronics, pp. 212–221, No. 658, Mar. 25, 1996.

Lemay, Laura, et al., "Approach of Java Language, Applet, AWT and Advanced Apparatus," First Edition, 22 pp. (translated), Aug. 20, 1996 (CS–NB–1999–00238–001).

Veldman, Franz, "Combating Viruses Heuristically," *Virus Bulletin Conference* 67–76, Sep. 1993.

Lo, Raymond W., et al., "Towards a Testbed for Malicious Code Detection," *Compcon Spring '91 Digest of Papers* at 160–166 (lEEE), 1991.

Lo, Raymond W., et al., "MCF: A Malicious Code Filter," 27 pp., May 4, 1994.

Polk, W. Timothy et al., "Anti–Virus Tools and Techniques for Computer Systems," Noyes Data Corporation, Park Ridge, New Jersey, pp. 12–27, Copyright 1995 (with cover and copyright pages—18 pp.).

Rasmusson, Andreas, et al., "Personal Security Assistance for Secure lnternet Commerce (Position Paper)," 12 pp., Available as dvi, ps, html, at http://www.sics.se/~ara/papers/NSP96.html, Sep. 16, 1996.

Le Charlier, Baudouin, et al., "Dynamic Detection and Classification of Computer Viruses Using General Behaviour Patterns," 22 pp., Jul. 2, 1995.

Lo, Raymond W., et al., "Towards a Testbed for Malicious Code Detection," from the Lawrence Livermore National Laboratory, 9 pp., Feb. 25—Mar. 1, 1991.

Martin, Jr., David M., "Blocking Java Applets at the Firewall," 11 pp., Available at http://www.cs.bu.edu/techreports/pdf/1996–026–java–firewalls.pdf (1997).

Skardhamar, Rune, "Virus: Detection and Elimination," Academic Press, lnc., pp. 33–48, Copyright 1996 (with cover and copyright page—18 pp.).

Hruska, Jan, "Computer Viruses and Anti–Virus Warfare (Second Revised Edition)," Ellis Horwood, pp. 87–95, Copyright 1992 (with cover and copyright page—11 pp.).

lS Tutorial Group 10–11, "Active Content Security," 35 pp., Dec. 13, 1999.

Stang, David J., "Computer Viruses and Artificial lntelligence," *Virus Bulletin Conference*, pp. 235–257, Sep. 1995.

Johannsen, Magnus, "Java Security and a Firewall Extension for Authenticity Control of Java Applets," Thesis Proposal, Computer Science Department, University of Colorado at Colorado Springs, 5 pp., Jan. 29, 1997.

Lo, Raymond, "Statis Analysis of Programs with Applications to Malicious Code Detection, Dissertation," 193 pp., 1992.

Marcionek, David, "A Complete ActiveX Web Control Tutorial," Available at http://www.codeproject.com/KB/COM/CompleteActiveX.aspx (2006).

Firewall Tookit (FWTK) 2.0 Beta Release, 1996.

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

NO AMENDMENTS HAVE BEEN MADE TO THE PATENT

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1**–**68** is confirmed.

* * * * *

US006480962B1

(12) United States Patent
Touboul

(10) Patent No.: **US 6,480,962 B1**
(45) Date of Patent: ***Nov. 12, 2002**

(54) **SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES**

(75) Inventor: **Shlomo Touboul**, Kefar-Haim (IL)

(73) Assignee: **Finjan Software, Ltd.**, Kefar-Haim (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/551,302**

(22) Filed: **Apr. 18, 2000**

Related U.S. Application Data

(63) Continuation of application No. 08/790,097, filed on Jan. 29, 1997.
(60) Provisional application No. 60/030,639, filed on Nov. 8, 1996.

(51) **Int. Cl.**^{7} **H02H 3/05**
(52) **U.S. Cl.** **713/200**; 713/201
(58) **Field of Search** 713/200, 201, 713/202; 714/38, 704; 709/225, 229

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,077,677	A	12/1991	Murphy et al.
5,359,659	A	10/1994	Rosenthal
5,361,359	A	11/1994	Tajalli et al.
5,485,409	A	1/1996	Gupta et al.
5,485,575	A	1/1996	Chess et al.
5,572,643	A	11/1996	Judson
5,606,668	A	2/1997	Shwed
5,623,600	A	4/1997	Ji et al.
5,638,446	A	6/1997	Rubin
5,692,047	A	11/1997	McManis
5,692,124	A	11/1997	Holden et al.
5,720,033	A	2/1998	Deo
5,724,425	A	3/1998	Chang et al.
5,740,248	A	4/1998	Fieres et al.
5,761,421	A	6/1998	van Hoff et al.

(List continued on next page.)

OTHER PUBLICATIONS

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990; pp. 21–29.
Okamoto, E. et al., "ID–Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013–5194, Jul. 19, 1990, Abstract and pp. 1169–1170. URL:http:/iel.ihs.com:80/cgi–bin/iel_cgi?se . . . 2ehts%26ViewTemplate%3ddocview%5fb%2ehts.
IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, Nov. 15, 1995, pp. 6–7.
Norvin Leach et al, "IE 3.0 Applets Will Earn Certification", PC Week, vol. 13, No. 29, Jul. 22, 1996, 2 pages.
"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software Ltd., Jul. 29, 1996, 1 page.

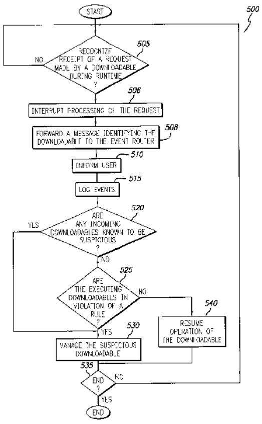
(List continued on next page.)

Primary Examiner—Dieu-Minh Le
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey, L.L.P.

(57) **ABSTRACT**

A system protects a client from hostile Downloadables. The system includes security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.

51 Claims, 7 Drawing Sheets


START
500
RECOGNIZE RECEIPT OF A REQUEST MADE BY A DOWNLOADABLE DURING RUNTIME ?
505
NO
INTERRUPT PROCESSING OF THE REQUEST
506
FORWARD A MESSAGE IDENTIFYING THE DOWNLOADABLE TO THE EVENT ROUTER
508
INFORM USER
510
LOG EVENTS
515
ARE ANY INCOMING DOWNLOADABLES KNOWN TO BE SUSPICIOUS ?
520
YES
NO
ARE THE EXECUTING DOWNLOADABLES IN VIOLATION OF A RULE ?
525
NO
YES
MANAGE THE SUSPICIOUS DOWNLOADABLE
530
RESUME OPERATION OF THE DOWNLOADABLE
540
535
END ?
NO
YES
END

Plaintiff's Trial Exhibit
PTX-2
Case No. 10-CV-00593-GMS

U.S. PATENT DOCUMENTS

5,765,205	A		6/1998	Breslau et al.	
5,784,459	A		7/1998	Devarakonda et al.	
5,796,952	A		8/1998	Davis et al.	
5,805,829	A		9/1998	Cohen et al.	
5,832,208	A		11/1998	Chen et al.	
5,850,559	A		12/1998	Angelo et al.	
5,859,966	A		1/1999	Hayman et al.	
5,864,683	A		1/1999	Boebert et al.	
5,892,904	A		4/1999	Atkinson et al.	
5,951,698	A		9/1999	Chen et al.	
5,956,481	A		9/1999	Walsh et al.	
5,974,549	A		10/1999	Golan	
5,983,348	A		11/1999	Ji	
6,092,194	A	*	7/2000	Touboul	713/200
6,154,844	A	*	11/2000	Touboul et al.	713/201
6,167,520	A	*	12/2000	Touboul	713/200

OTHER PUBLICATIONS

"Powerful PC Security for the New World of JAVA™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996, including Abstract, Contents, Introduction and pp. 1–10.

"Finjan Announces a Personal Java™ Firewall For Web Browsers—the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, Oct. 21, 1996, 2 pages.

Company Profile "Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Article published on the Internet, 7 pages.

Mark LaDue, "Online Business Consultant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.

Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated Feb. 17, 1997, Printed Dec. 23, 1998. URL: http://www.microsoft-.com/workshop/security/authcode/signfaq.asp#9, pp. 1–13.

Zhang, X.N., "Secure Code Distribution", IEEE/IEE Electronic Library online, Computer, vol. 30, Issue 6, Jun. 1997, pp.: 76–79.

* cited by examiner

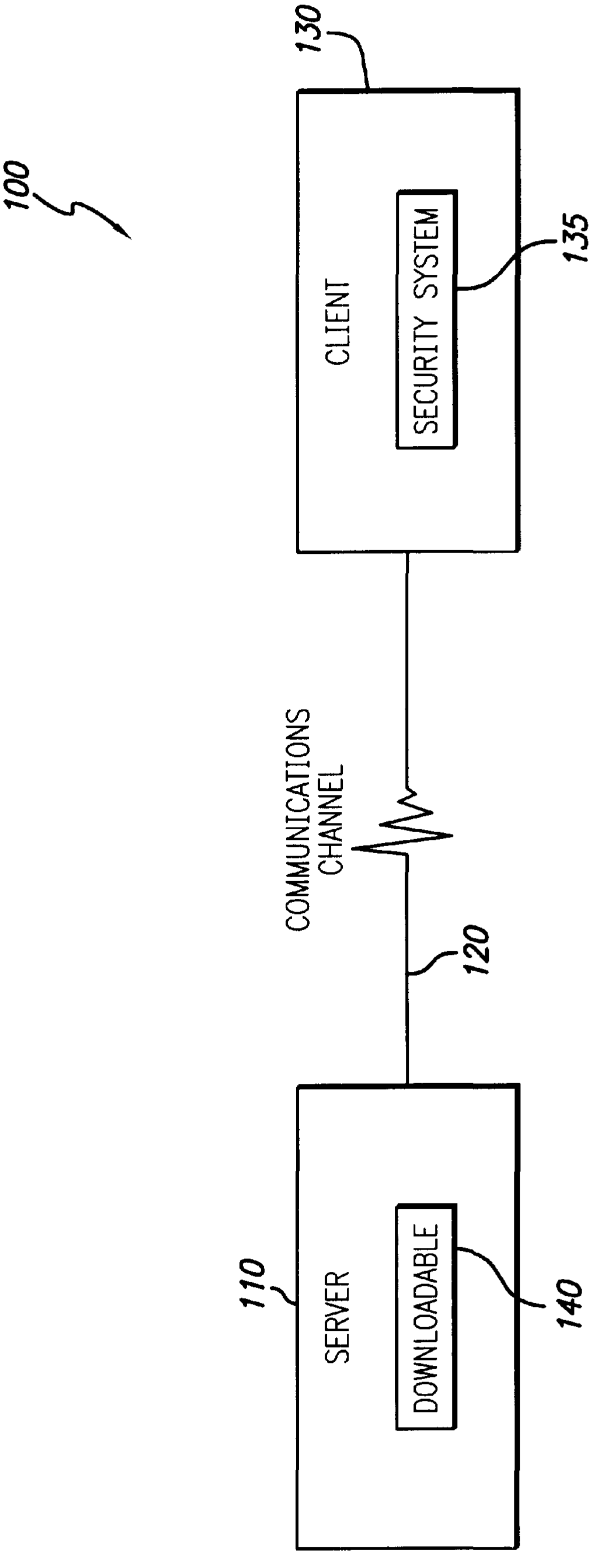

100
130
CLIENT
SECURITY SYSTEM
135
COMMUNICATIONS CHANNEL
120
110
SERVER
DOWNLOADABLE
140

FIG. 1

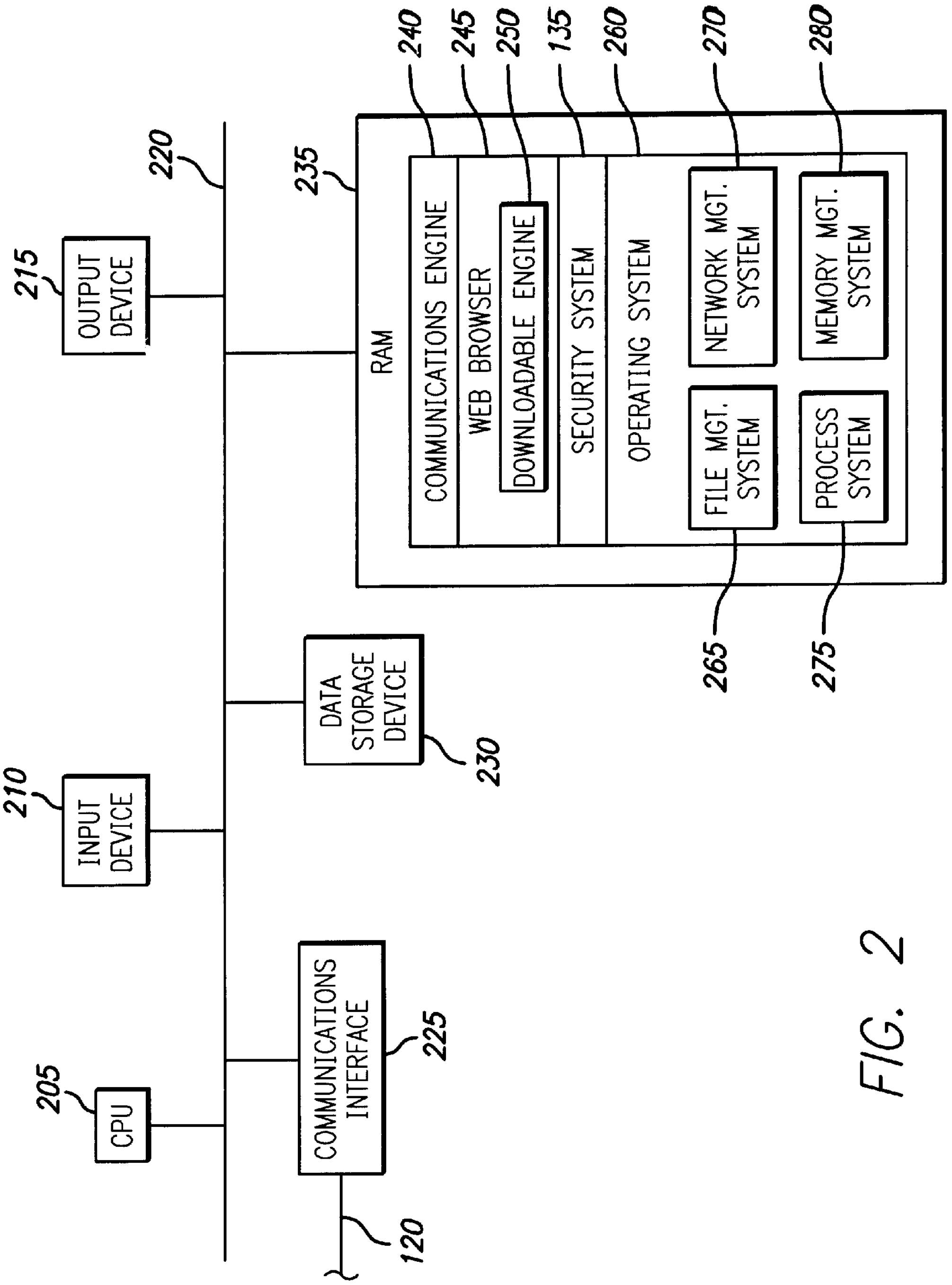

215
OUTPUT DEVICE
220
235
RAM
240
245
250
135
260
270
280
COMMUNICATIONS ENGINE
WEB BROWSER
DOWNLOADABLE ENGINE
SECURITY SYSTEM
OPERATING SYSTEM
NETWORK MGT. SYSTEM
MEMORY MGT. SYSTEM
FILE MGT. SYSTEM
PROCESS SYSTEM
265
275
DATA STORAGE DEVICE
230
210
INPUT DEVICE
205
CPU
COMMUNICATIONS INTERFACE
225
120

FIG. 2

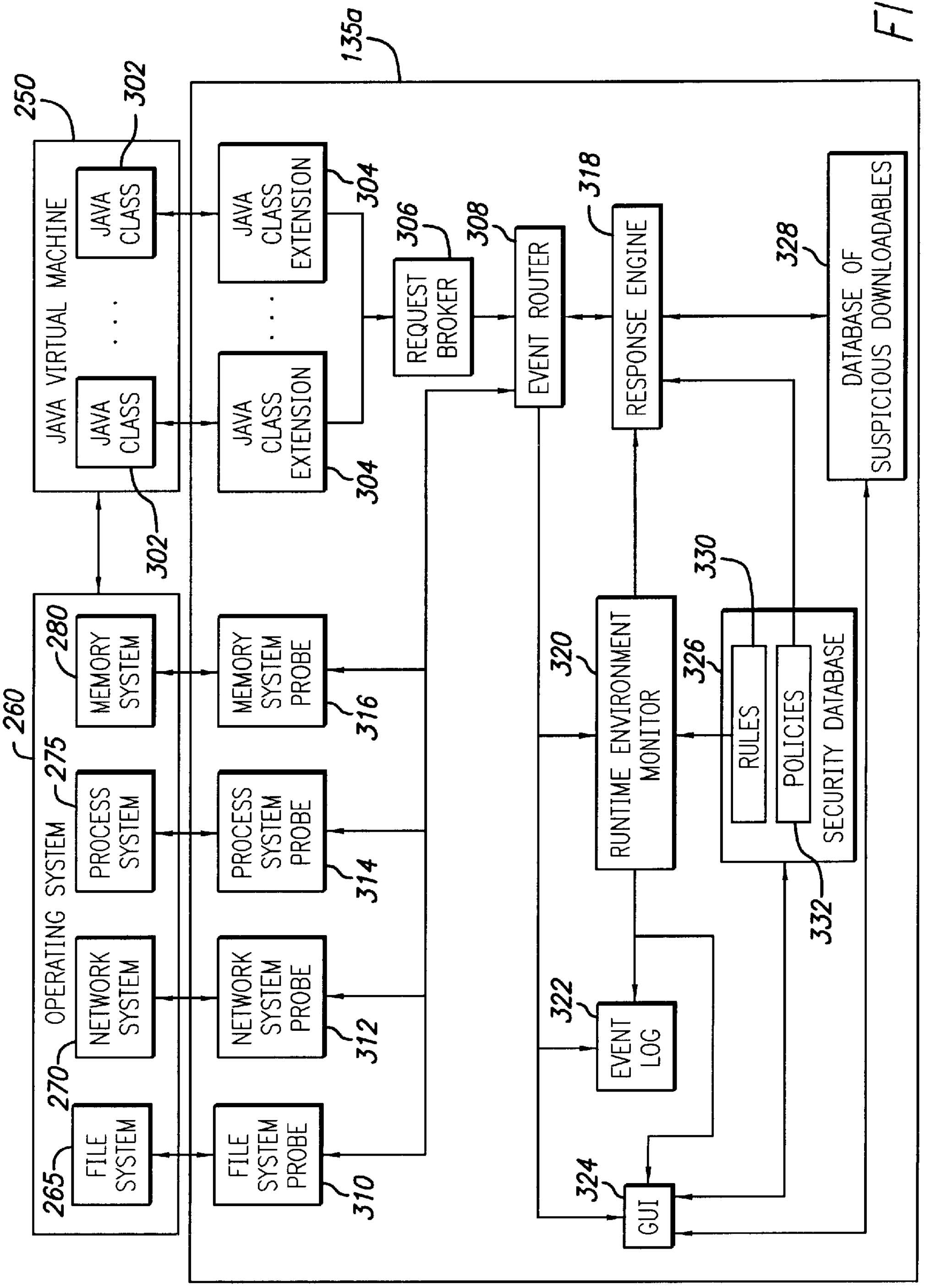

135a
250
JAVA VIRTUAL MACHINE
JAVA CLASS
302
JAVA CLASS
302
. . .
JAVA CLASS EXTENSION
304
JAVA CLASS EXTENSION
304
. . .
306
REQUEST BROKER
308
EVENT ROUTER
318
RESPONSE ENGINE
328
DATABASE OF SUSPICIOUS DOWNLOADABLES
260
OPERATING SYSTEM
280
MEMORY SYSTEM
275
PROCESS SYSTEM
270
NETWORK SYSTEM
265
FILE SYSTEM
MEMORY SYSTEM PROBE
316
PROCESS SYSTEM PROBE
314
NETWORK SYSTEM PROBE
312
FILE SYSTEM PROBE
310
320
RUNTIME ENVIRONMENT MONITOR
330
326
RULES
POLICIES
SECURITY DATABASE
332
322
EVENT LOG
324
GUI

FIG. 3

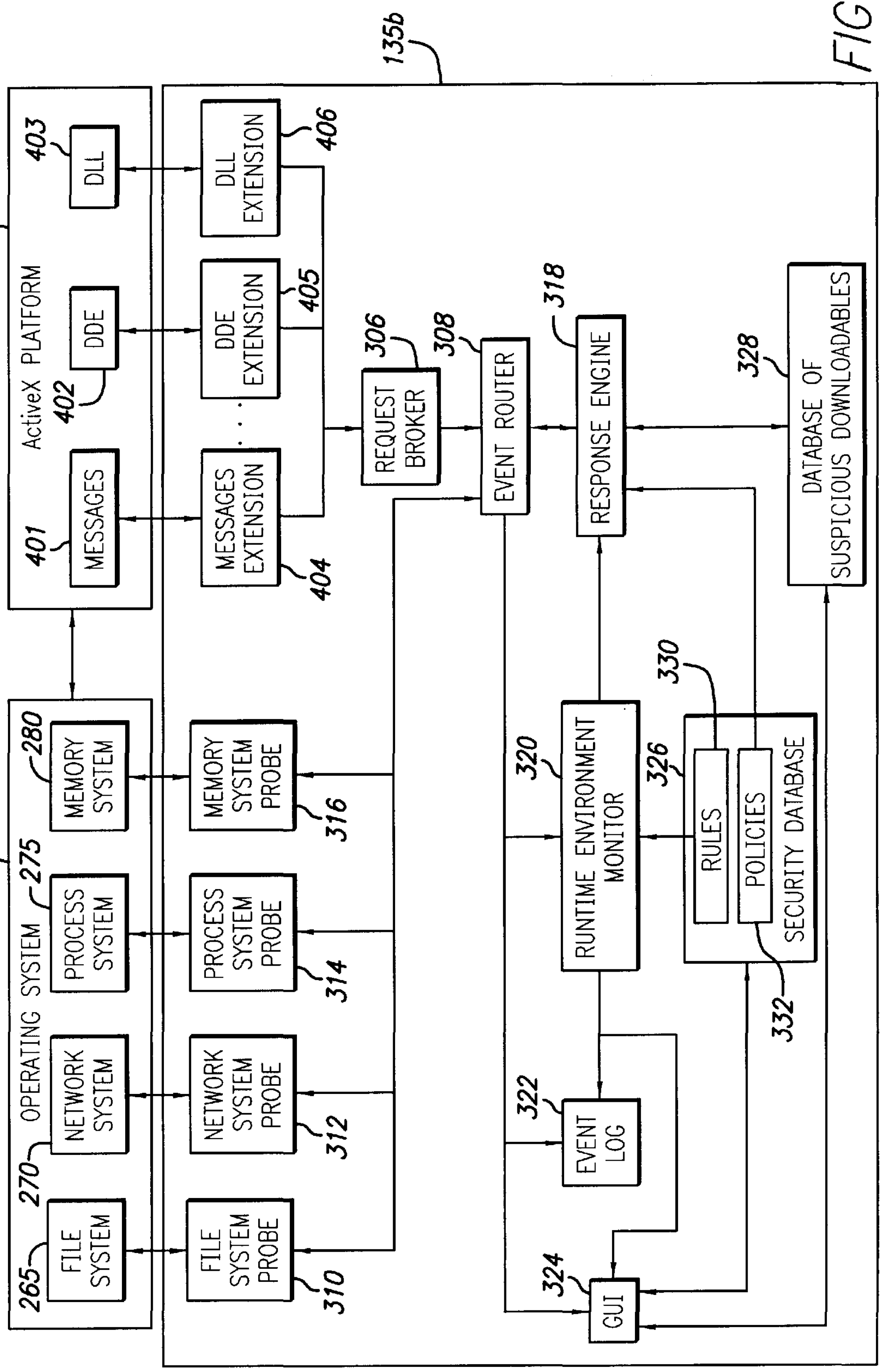

135b
250
ActiveX PLATFORM
401
MESSAGES
402
DDE
403
DLL
404
MESSAGES EXTENSION
405
DDE EXTENSION
406
DLL EXTENSION
306
REQUEST BROKER
308
EVENT ROUTER
318
RESPONSE ENGINE
328
DATABASE OF SUSPICIOUS DOWNLOADABLES
260
OPERATING SYSTEM
265
FILE SYSTEM
270
NETWORK SYSTEM
275
PROCESS SYSTEM
280
MEMORY SYSTEM
310
FILE SYSTEM PROBE
312
NETWORK SYSTEM PROBE
314
PROCESS SYSTEM PROBE
316
MEMORY SYSTEM PROBE
320
RUNTIME ENVIRONMENT MONITOR
322
EVENT LOG
324
GUI
326
330
RULES
332
POLICIES
SECURITY DATABASE

FIG. 4

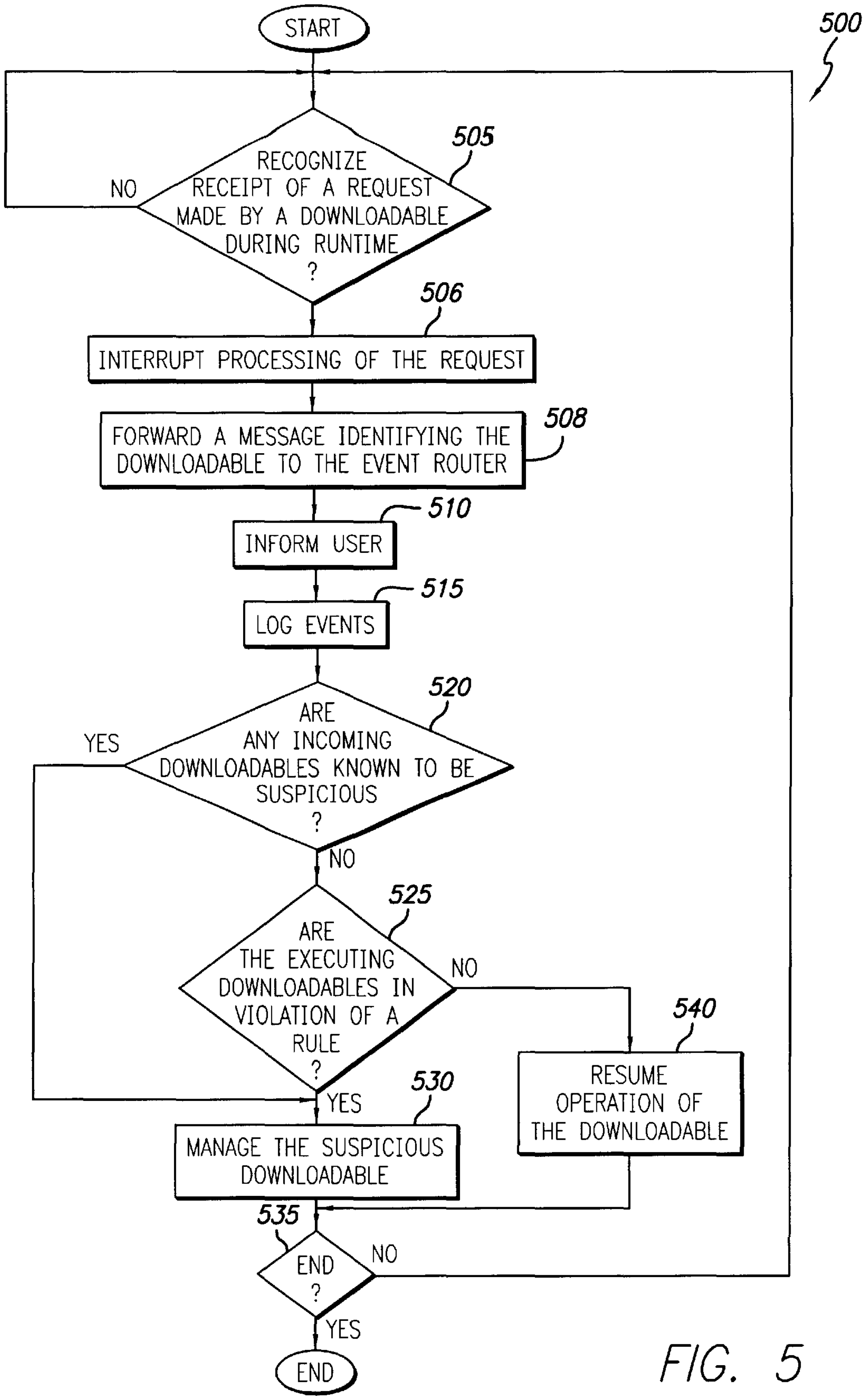

START
500
RECOGNIZE RECEIPT OF A REQUEST MADE BY A DOWNLOADABLE DURING RUNTIME ?
505
NO
506
INTERRUPT PROCESSING OF THE REQUEST
FORWARD A MESSAGE IDENTIFYING THE DOWNLOADABLE TO THE EVENT ROUTER
508
INFORM USER
510
LOG EVENTS
515
ARE ANY INCOMING DOWNLOADABLES KNOWN TO BE SUSPICIOUS ?
520
YES
NO
ARE THE EXECUTING DOWNLOADABLES IN VIOLATION OF A RULE ?
525
NO
YES
RESUME OPERATION OF THE DOWNLOADABLE
540
MANAGE THE SUSPICIOUS DOWNLOADABLE
530
535
END ?
NO
YES
END

FIG. 5

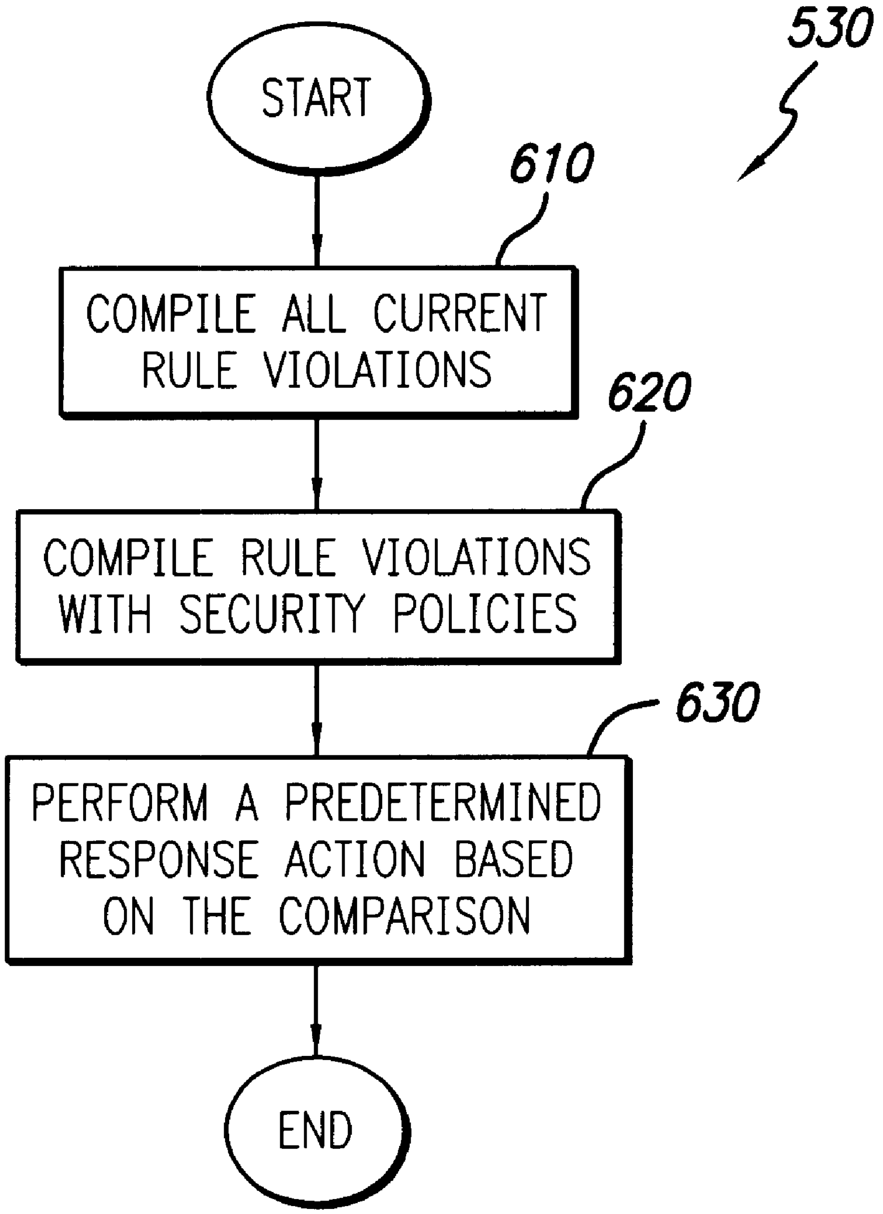

530
START
610
COMPILE ALL CURRENT RULE VIOLATIONS
620
COMPILE RULE VIOLATIONS WITH SECURITY POLICIES
630
PERFORM A PREDETERMINED RESPONSE ACTION BASED ON THE COMPARISON
END

FIG. 6

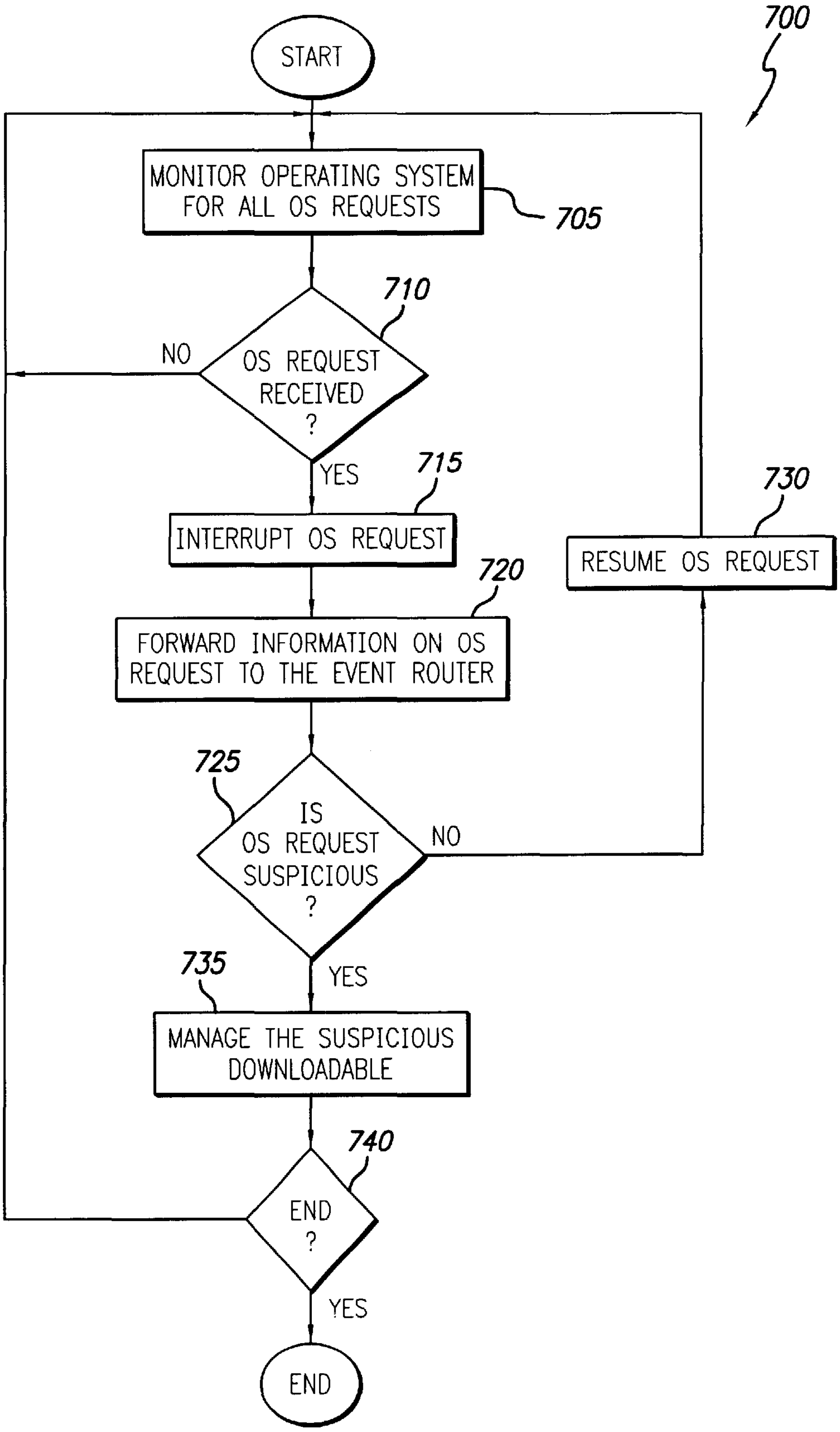

700
START
MONITOR OPERATING SYSTEM FOR ALL OS REQUESTS
705
710
OS REQUEST RECEIVED ?
NO
YES
715
INTERRUPT OS REQUEST
720
FORWARD INFORMATION ON OS REQUEST TO THE EVENT ROUTER
730
RESUME OS REQUEST
725
IS OS REQUEST SUSPICIOUS ?
NO
YES
735
MANAGE THE SUSPICIOUS DOWNLOADABLE
740
END ?
YES
END

FIG. 7

SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to co-pending provisional patent application filed on Nov. 8, 1996, entitled "System and Method for Protecting a Computer from Hostile Downloadables," Ser. No. 60/030,639, by inventor Shlomo Touboul, and is a continuation of U.S. patent application filed on Jan. 29, 1997, entitled "System and Method for Protecting a Computer During Runtime From Hostile Downloadbales," Ser. No. 08/790,097, by inventor Shlomo Touboul, which subject matters are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly to a system and method for protecting clients from hostile Downloadables.

2. Description of the Background Art

The Internet currently interconnects about 100,000 individual computer networks and several million computers. Because it is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

In response to the widespread generation and distribution of computer viruses, programmers continue to design and update security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are typically not configured to recognize computer viruses which have been attached to or masked as harmless Downloadables (i.e., applets). A Downloadable is a small executable or interpretable application program which is downloaded from a source computer and run on a destination computer. A Downloadable is used in a distributed environment such as in the Java™ distributed environment produced by Sun Microsystems or in the ActiveX™ distributed environment produced by Microsoft Corporation.

Hackers have developed hostile Downloadables designed to penetrate security holes in Downloadable interpreters. In response, Sun Microsystems, Inc. has developed a method of restricting Downloadable access to resources (file system resources, operating system resources, etc.) on the destination computer, which effectively limits Downloadable functionality at the Java™ interpreter. Sun Microsystems, Inc. has also provided access control management for basing Downloadable-accessible resources on Downloadable type. However, the above approaches are difficult for the ordinary web surfer to manage, severely limit Java™ performance and functionality, and insufficiently protect the destination computer.

Other security system designers are currently considering digital signature registration stamp techniques, wherein, before a web browser will execute a Downloadable, the Downloadable must possess a digital signature registration stamp. Although a digital signature registration stamp will diminish the threat of Downloadables being intercepted, exchanged or corrupted, this approach only partially addresses the problem. This method does not stop a hostile Downloadable from being stamped with a digital signature, and a digital signature does not guarantee that a Downloadable is harmless. Therefore, a system and method are needed for protecting clients from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a client from hostile Downloadables. The system includes security rules defining suspicious actions such as WRITE operations to a system configuration file, overuse of system memory, overuse of system processor time, etc. and security policies defining the appropriate responsive actions to rule violations such as terminating the applet, limiting the memory or processor time available to the applet, etc. The system includes an interface, such as Java™ class extensions and operating system probes, for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing the violation-based responsive action.

The present invention further provides a method for protecting a client from hostile Downloadables. The method includes the steps of recognizing a request made by a Downloadable during runtime, interrupting processing of the request, comparing information pertaining to the Downloadable against a predetermined security policy, recording all rule violations in a log, and performing a predetermined responsive action based on the comparison.

It will be appreciated that the system and method of the present invention use at least three hierarchical levels of security. A first level examines the incoming Downloadables against known suspicious Downloadables. A second level examines runtime events. A third level examines the Downloadables operating system requests against predetermined suspicious actions. Thus, the system and method of the invention are better able to locate hostile operations before client resources are damaged.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating a network system in accordance with the present invention;

FIG. **2** is a block diagram illustrating details of the client;

FIG. **3** is a block diagram illustrating details of a security system;

FIG. **4** is a block diagram illustrating details of an alternative security system;

FIG. **5** is a flowchart illustrating a method for protecting a client from suspicious Downloadables;

FIG. **6** is a flowchart illustrating the method for managing a suspicious Downloadable; and

FIG. **7** is a flowchart illustrating a supplementary method for protecting a client from suspicious Downloadables.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a block diagram illustrating a network system **100** in accordance with the present invention. Network system **100** includes a server **110** coupled to a communications channel **120**, e.g., an Internet or an Intranet. The communications channel **120** is in turn coupled to a client **130**, e.g., an individual computer, a network computer, a kiosk workstation, etc., which includes a security system

135 for protecting the client **130** from hostile (i.e., will adversely effect the operational characteristics of the client **130**) or suspicious (i.e., potentially hostile) downloadables.

Server **110** forwards a Downloadable **140** across the communications channel **120** to the client **130**. During runtime, the security system **135** examines each Downloadable **140** and the actions of each Downloadable **140** to monitor for hostile or suspicious actions.

FIG. **2** is a block diagram illustrating details of a client **130**, which includes a Central Processing Unit (CPU) **205**, such as a Motorola Power PC® microprocessor or an Intel Pentium® microprocessor, coupled to a signal bus **220**. The client **130** further includes an input device **210** such as a keyboard and mouse, an output device **215** such as a Cathode Ray Tube (CRT) display, a data storage device **230** such as Read Only Memory (ROM) or magnetic disk, and a Random-Access Memory (RAM) **235**, each being coupled to signal bus **220**. A communications interface **225** is coupled between the communications channel **120** and the signal bus **220**.

An operating system **260** controls processing by CPU **205**, and is typically stored in data storage device **230** and loaded into RAM **235** for execution. The operating system **260** includes a file management system **265**, a network management system **270**, a process system **275** for controlling CPU **205**, and a memory management system **280** for controlling memory use and allocation. A communications engine **240** generates and transfers message packets to and from the communications channel **140** via the communications interface **225**, and may also be stored in data storage device **230** and loaded into RAM **235** for execution.

The client **130** further includes a web browser **245**, such as the Netscape™ web browser produced by the Netscape Corporation, the Internet Explorer™ web browser produced by the Microsoft Corporation, or the Java™ Developers Kit 1.0 web browser produced by Sun Microsystems, Inc., for communicating via the communications channel **120**. The web browser **245** includes a Downloadable engine **250** for managing and executing received Downloadables **140**.

The client **130** further includes the security system **135** as described with reference to FIG. **1**. The security system **135** may be stored in data storage device **230** and loaded into RAM **235** for execution. During runtime, the security system **135** intercepts and examines Downloadables **140** and the actions of Downloadables **140** to monitor for hostile or suspicious actions. If the security system **135** recognizes a suspicious Downloadable **140** or a suspicious request, then the security system **135** can perform an appropriate responsive action such as terminating execution of the Downloadable **140**.

FIG. **3** is a block diagram illustrating details of the security system **135***a*, which is a first embodiment of security system **135** of FIG. **2** when operating in conjunction with a Java™ virtual machine **250** (i.e., the Downloadable engine **250**) that includes conventional Java™ classes **302**. Each of the Java™ classes **302** performs a particular service such as loading applets, managing the network, managing file access, etc. Although applets are typically described with reference to the Java™ distributed environment, applets herein correspond to all downloadable executable or interpretable programs for use in any distributed environment such as in the ActiveX™ distributed environment.

Examples of Java™ classes used in Netscape Navigator™ include AppletSecurity.class, EmbeddedAppletFrame.class:, AppletClassLoader.class, MozillaAppletContext.class, ServerSocket.class, SecurityException.class and SecurityManager.class, etc. Examples of Java™ classes used in Internet Explorer™ include AppletSecurity.class, BrowserAppletFrame.class, AppletClassLoader.class, ServerSocket.class, SecurityException.class and SecurityManager.class, etc. Other classes may include Broker.class, BCInterface.class, SocketConnection.class, queueManager.class, BrowserExtension.class, Message.class, MemoryMeter.class and AppletDescription-.class.

The security system **135***a* includes Java™ class extensions **304**, wherein each extension **304** manages a respective one of the Java™ classes **302**. When a new applet requests the service of a Java class **302**, the corresponding Java™ class extension **304** interrupts the request and generates a message to notify the request broker **306** of the Downloadable's request. The request broker **306** uses TCP/IP message passing protocol to forward the message to the event router **308**.

The security system **135***a* further includes operating system probes **310**, **312**, **314** and **316**. More particularly, a file management system probe **310** recognizes applet instructions sent to the file system **265** of operating system **260**, a network system probe **312** recognizes applet instructions set to the network management system **270** of operating system **260**, a process system probe **314** recognizes applet instructions sent to the process system **275** of operating system **260**, and a memory management system probe **316** recognizes applet instructions sent to the memory system **280** of operating system **260**. When any of the probes **310**–**316** recognizes an applet instruction, the recognizing probe **310**–**316** sends a message to inform the event router **308**.

Upon receipt of a message, the event router **308** accordingly forwards the message to a Graphical User Interface (GUI) **324** for notifying the user of the request, to an event log **322** for recording the message for subsequent analysis, and to a runtime environment monitor **320** for determining whether the request violates a security rule **330** stored in a security database **326**. Security rules **330** include a list of computer operations which are deemed suspicious. Suspicious operations may include READ/WRITE operations to a system configuration file, READ/WRITE operations to a document containing trade secrets, overuse of system memory, overuse of system processor time, too many applets running concurrently, or too many images being displayed concurrently. For example, the runtime environment monitor **320** may determine that a security rule **330** has been violated when it determines that an applet uses more than two megabytes of RAM **235** or when the Java™ virtual machine **250** runs more than five applets concurrently.

Upon recognition of a security rule **330** violation, the runtime environment monitor **320** records the violation with the event log **322**, informs the user of the violation via the GUI **324** and forwards a message to inform the response engine **318** of the violation. The response engine **318** analyzes security policies **332** stored in the security database **326** to determine the appropriate responsive action to the rule **330** violation. Appropriate responsive actions may include terminating the applet, limiting the memory or processor time available to the applet, etc. For example, the response engine **318** may determine that a security policy **332** dictates that when more than five applets are executed concurrently, operation of the applet using the greatest amount of RAM **235** should be terminated. Further, a security policy **332** may dictate that when an applet or a combination of applets violates a security policy **332**, the response engine **318** must add information pertaining to the applet or applets to the suspicious Downloadables database

328. Thus, when the applet or applets are encountered again, the response engine **318** can stop them earlier.

The GUI **324** enables a user to add or modify the rules **330** of the security database **326**, the policies **332** of the security database **326** and the suspicious applets of the suspicious Downloadables database **328**. For example, a user can use the GUI **324** to add to the suspicious Downloadables database **328** applets generally known to be hostile, applets deemed to be hostile by the other clients **130** (not shown), applets deemed to be hostile by network MIS managers, etc. Further, a user can use the GUI **324** to add to the rules **330** actions generally known to be hostile, actions deemed to be hostile by network MIS managers, etc.

It will be appreciated that the embodiment illustrated in FIG. **3** includes three levels of security. The first level examines the incoming Downloadables **140** against known suspicious Downloadables. The second level examines the Downloadables'access to the Java™ classes **302**. The third level examines the Downloadables requests to the operating system **260**. Thus, the security system **135***a* is better apt to locate a hostile operation before an operation damages client **130** resources.

FIG. **4** is a block diagram illustrating details of a security system **135***b*, which is a second embodiment of security system **135** when operating in conjunction with the ActiveX™ platform (i.e., the Downloadable engine **250**) which uses message **401** calls, Dynamic-Data-Exchange (DDE) **402** calls and Dynamically-Linked-Library (DLL) **403** calls. Thus, instead of having Java™ class extensions **304**, the security system **135** has a messages extension **401** for recognizing message **401** calls, a DDE extension **405** for recognizing DDE **402** calls and a DLL extension **406** for recognizing DLL calls. Upon recognition of a call, each of the messages extension **404**, the DDE extension **405** and the DLL extension **406** send a message to inform the request broker **306**. The request broker **306** and the remaining elements operate similarly to the elements described with reference to FIG. **3**.

FIG. **5** is a flowchart illustrating a method **500** for protecting a client **130** from hostile and suspicious Downloadables **140**. Method **500** begins with the extensions **304**, **404**, **405** or **406** in step **505** waiting to recognize the receipt of a request made by a Downloadable **140**. Upon recognition of a request, the recognizing extension **304**, **404**, **405** or **406** in step **506** interrupts processing of the request and in step **508** generates and forwards a message identifying the incoming Downloadable **140** to the request broker **306**, which forwards the message to the event router **308**.

The event router **308** in step **510** forwards the message to the GUI **324** for informing the user and in step **515** to the event log **322** for recording the event. Further, the event router **308** in step **520** determines whether any of the incoming Downloadables **140** either alone or in combination are known or previously determined to be suspicious. If so, then method **500** jumps to step **530**. Otherwise, the runtime environment monitor **320** and the response engine **318** in step **525** determine whether any of the executing Downloadables **140** either alone or in combination violate a security rule **330** stored in the security database **332**.

If a rule **330** has been violated, then the response engine **318** in step **530** manages the suspicious Downloadable **140**. Step **530** is described in greater detail with reference to FIG. **6**. Otherwise, if a policy has not been violated, then response engine **318** in step **540** resumes operation of the Downloadable **140**. In step **535**, a determination is made whether to end method **500**. For example, if the user disconnects the client **130** from the server **110**, method **500** ends. If a request to end is made, then method **500** ends. Otherwise, method **500** returns to step **505**.

FIG. **6** is a flowchart illustrating details of step **530**. Since multiple rule **330** violations may amount to a more serious violation and thus require a stricter response by the response engine **318**, step **530** begins with the response engine **318** in step **610** compiling all rule **330** violations currently occurring. The response engine **318** in step **620** compares the compiled rule **330** violations with the security policies **332** to determine the appropriate responsive action for managing the suspicious Downloadable **140** or Downloadables **140**, and in step **630** the response engine **318** performs a predetermined responsive action. Predetermined responsive actions may include sending a message via the GUI **324** to inform the user, recording the message in the event log **322**, stopping execution of a suspicious Downloadable **140**, storing a Downloadable **140** or combination of Downloadables **140** in the suspicious Downloadable database **328**, limiting memory available to the Downloadable **140**, limiting processor time available to the Downloadable **140**, etc.

FIG. **7** is a flowchart illustrating a supplementary method **700** for protecting a client **130** from suspicious Downloadables **140**. Method **700** begins with operating system probes **310**, **312**, **314** and **316** in step **705** monitoring the operating system **260** for Operating System (OS) requests from Downloadables **140**. As illustrated by step **710**, when one of the probes **310–316** recognizes receipt of an OS request, the recognizing probe **310–316** in step **715** interrupts the request and in step **720** forwards a message to inform the event router **308**.

The event router **308** in step **725** routes the information to each of the components of the security engine **135** as described with reference to FIG. **5**. That is, the event router **308** forwards the information to the GUI **324** for informing the user, to the event log **322** for recordation and to the runtime environment monitor **320** for determining if the OS request violates a rule **330**. The response engine **318** compares the OS request alone or in combination with other violations against security policies **332** to determine the appropriate responsive actions. It will be appreciated that, based on the security policies **332**, the response engine **318** may determine that an OS request violation in combination with other OS request violations, in combination with rule **330** violations, or in combination with both other OS request violations and rule **330** violations merits a stricter responsive action.

If the OS request does not violate a security rule **330**, then the response engine **318** in step **730** instructs the operating system **260** via the recognizing probe **310–316** to resume operation of the OS request. Otherwise, if the OS request violates a security rule **330**, then the response engine **318** in step **730** manages the suspicious Downloadable by performing the appropriate predetermined responsive actions as described with reference to FIGS. **5** and **6**. In step **740**, a determination is made whether to end method **700**. If a request to end the method is made, then method **700** ends. Otherwise, method **700** returns to step **705**.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method, comprising:

monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison.

2. The method of claim **1**, wherein monitoring the operating system includes monitoring a request sent to a Downloadable engine.

3. The method of claim **2**,

wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and

wherein monitoring the operating system includes monitoring each Java™ class for receipt of the request.

4. The method of claim **2**,

wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and

wherein monitoring the operating system includes monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

5. The method of claim **1**, further comprising determining whether information pertaining to the Downloadable violates a security rule.

6. The method of claim **5**, further comprising determining whether violation of the security rule violates the security policy.

7. The method of claim **1**, further comprising:

comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable; and

performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

8. The method of claim **1**, wherein the predetermined responsive action includes storing results of the comparison in an event log.

9. The method of claim **1**, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

10. The method of claim **1**, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

11. The method of claim **1**, wherein the predetermined responsive action includes discarding the Downloadable.

12. A system, comprising:

a security policy;

a plurality of operating system interfaces operating substantially in parallel, each interface for recognizing a runtime event in a subsystem of the operating system caused from a request made by a Downloadable;

a first comparator coupled to the interfaces for comparing information pertaining to the received Downloadable with the security policy; and

a response engine coupled to the first comparator for performing a predetermined responsive action based on the comparison with the security policy.

13. The system of claim **12**, wherein the interfaces-include a Java™ class extension for monitoring a Java™ class in a Java™ virtual machine for receipt of a request.

14. The system of claim **12**, wherein the interfaces include an AppletX™ extension for monitoring a message engine, a dynamic-data-exchange and a dynamically-linked library in an AppletX™ environment for receipt of a request.

15. The system of claim **12**, further comprising

a security rule; and

a second comparator, coupled to the interfaces and to the response engine, for determining whether information pertaining to the Downloadable violates the security rule.

16. The system of claim **15**, wherein the first comparator determines whether violation of the security rule violates the security policy.

17. The system of claim **12**, further comprising

a predetermined suspicious Downloadable; and

a second comparator coupled to the interfaces for comparing information pertaining to the Downloadable with information pertaining to the predetermined suspicious Downloadable;

wherein the response engine is further coupled to the second comparator and performs the responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

18. The system of claim **12**, further comprising an event log coupled to the first comparator for storing results of the comparison.

19. The system of claim **12**, further comprising a user interface coupled to the first comparator.

20. The system of claim **12**, further comprising a suspicious Downloadable database for storing information on known and previously-deemed suspicious Downloadables.

21. The system of claim **12**, wherein the predetermined suspicious action includes discarding the Downloadable.

22. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:

means for monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;

means for interrupting processing of the request;

means for comparing information pertaining to the Downloadable against a predetermined security policy; and

means for performing a predetermined responsive action based on the comparison.

23. The system of claim **22**, wherein the means for monitoring the operating system includes means for monitoring a request sent to a Downloadable engine.

24. The system of claim **23**,

wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and

wherein the means for monitoring the operating system includes means for monitoring each Java™ class for receipt of the request.

25. The system of claim **23**,

wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and

wherein the means for monitoring the operating system includes means for monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

26. The system of claim 22, further comprising means for determining whether information pertaining to the Downloadable violates a security rule.

27. The system of claim 26, further comprising means for determining whether violation of the security rule violates the security policy.

28. The method of claim 22, further comprising:

means for comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable; and

means for performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

29. The system of claim 22, wherein the predetermined responsive action includes storing results of the comparison in an event log.

30. The system of claim 22, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

31. The system of claim 22, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

32. The system of claim 22, wherein the predetermined responsive action includes discarding the Downloadable.

33. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison.

34. The medium of claim 33, wherein monitoring the operating system includes monitoring a request sent to a Downloadable engine.

35. The medium of claim 33,

wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and

wherein monitoring the operating system includes monitoring each Java™ class for receipt of the request.

36. The medium of claim 35,

wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and

wherein monitoring the operating system includes monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

37. The medium of claim 33, further comprising determining whether information pertaining to the Downloadable violates a security rule.

38. The medium of claim 37, further comprising determining whether violation of the security rule violates the security policy.

39. The medium of claim 33, further comprising:

comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable; and

performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

40. The medium of claim 33, wherein the predetermined responsive action includes storing results of the comparison in an event log.

41. The medium of claim 33, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

42. The medium of claim 33, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

43. The medium of claim 33, wherein the predetermined responsive action includes discarding the Downloadable.

44. The system of claim 1, wherein each subsystem includes one of a file system, network system, process system or memory system.

45. The system of claim 12, wherein each subsystem includes one of a file system, network system, process system or memory system.

46. The system of claim 22, wherein each subsystem includes one of a file system, network system, process system or memory system.

47. The system of claim 33, wherein each subsystem includes one of a file system, network system, process system or memory system.

48. A method, comprising:

intercepting, by an operating system probe associated with an operating system function, an operating system call being issued by a downloadable to an operating system and associated with the operating system function;

comparing, by a runtime environment monitor, the operating system call against a predetermined security policy before allowing the operating system to process the operating system call;

blocking, by a response engine, operating system calls that are forbidden according to the security policy; and

allowing, by the response engine, operating system calls that are permitted according to the security policy.

49. The method of claim 48, wherein the Downloadable is one of a Java component, an ActiveX control, executable code, or interpretable code.

50. A system, comprising:

an operating system probe associated with an operating system function for intercepting an operating system call being issued by a downloadable to an operating system and associated with the operating system function;

a runtime environment monitor for comparing the operating system call against a predetermined security policy before allowing the operating system to process the operating system call; and

a response engine for blocking operating system calls that are forbidden according to the security policy, and for allowing operating system calls that are permitted according to the security policy.

51. The system of claim 50, wherein the Downloadable is one of a Java component, an ActiveX control, executable code, or interpretable code.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 6,480,962 B1	Page 1 of 1
APPLICATION NO.	: 09/551302	
DATED	: November 12, 2002	
INVENTOR(S)	: Touboul, Shlomo	

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Col. 7, 8 and 9;
On pages 13 and 14 in Claims 4, 25 and 36, and in two places on page 13 in Claim 14, the term "AppletX" was erroneously typed instead of the correct term "ActiveX". The term "ActiveX" appears in the Specification in Column 1 on Line 44, in Column 3 on Line 63 and in Column 5 on Line 26

Signed and Sealed this

First Day of August, 2006

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office

US006480962C1

(12) EX PARTE REEXAMINATION CERTIFICATE (6842nd)

United States Patent (10) **Number: US 6,480,962 C1**
Touboul (45) **Certificate Issued: *May 26, 2009**

(54) **SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES**

(75) Inventor: **Shlomo Touboul**, Kefar-Haim (IL)

(73) Assignee: **Finjan Software, Ltd.**, Kefar-Haim (IL)

Reexamination Request:
No. 90/008,678, Jun. 6, 2007

Reexamination Certificate for:

Patent No.:	**6,480,962**
Issued:	**Nov. 12, 2002**
Appl. No.:	**09/551,302**
Filed:	**Apr. 18, 2000**

(*) Notice: This patent is subject to a terminal disclaimer.

Certificate of Correction issued Aug. 7, 2006.

Related U.S. Application Data

(63) Continuation of application No. 08/790,097, filed on Jan. 29, 1997, now Pat. No. 6,167,520.

(60) Provisional application No. 60/030,639, filed on Nov. 8, 1996.

(51) **Int. Cl.**

G06F 11/00	(2006.01)
H02H 03/05	(2006.01)
G06F 12/00	(2006.01)

(52) **U.S. Cl.** **726/22**; 709/223; 709/224; 726/24

(58) **Field of Classification Search** 726/22; 709/223
See application file for complete search history.

(56) **References Cited**

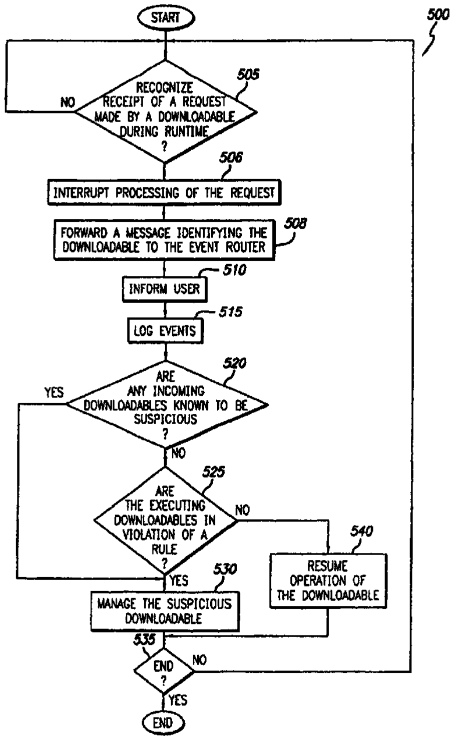
PUBLICATIONS

Endrijonas, Janet, "Rx PC The Anti–Virus Handbook," TAB Books, 1993 (185 pages).
Binstock, Andrew, "Multithreading, Hyper–threading, Multiprocessing: Now, what's the difference?" http://www.intel.com/cd/ids/developer/asmo–na/eng/20456.htm, Pacific Data Works, LLC, downloaded Jul. 7, 2008 (7 pages).

Primary Examiner—Anil Khatri

(57) **ABSTRACT**

A system protects a client from hostile Downloadables. The system includes security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.


START
500
RECOGNIZE RECEIPT OF A REQUEST MADE BY A DOWNLOADABLE DURING RUNTIME ?
505
NO
506
INTERRUPT PROCESSING OF THE REQUEST
FORWARD A MESSAGE IDENTIFYING THE DOWNLOADABLE TO THE EVENT ROUTER
508
INFORM USER
510
LOG EVENTS
515
ARE ANY INCOMING DOWNLOADABLES KNOWN TO BE SUSPICIOUS ?
520
YES
NO
ARE THE EXECUTING DOWNLOADABLES IN VIOLATION OF A RULE ?
525
NO
YES
540
RESUME OPERATION OF THE DOWNLOADABLE
MANAGE THE SUSPICIOUS DOWNLOADABLE
530
535
END ?
NO
YES
END

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1**, **2**, **5**–**12**, **15**–**23**, **26**–**34**, **37**–**48** and **50** is confirmed.

New claims **52**–**55** are added and determined to be patentable.

Claims **3**, **4**, **13**, **14**, **24**, **25**, **35**, **36**, **49** and **51** were not reexamined.

52. A computer-based method, comprising:

monitoring substantially in parallel a plurality of subsystems of an operating system during runtime for an event caused from a request made by a Downloadable, wherein the plurality of subsystems includes a network system;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison.

53. A computer-based method, comprising:

monitoring substantially in parallel a plurality of subsystems of an operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy, wherein information pertaining to the Downloadable includes information about requests to the operating system made by the Downloadable; and

performing a predetermined responsive action based on the comparison.

54. A computer-based method, comprising:

monitoring substantially in parallel a plurality of subsystems of an operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the downloadable against a predetermined security policy, wherein information pertaining to the Downloadable includes information about memory usage by the Downloadable; and

performing a predetermined responsive action based on the comparison.

55. A computer-based method, comprising:

monitoring substantially in parallel a plurality of subsystems of an operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, wherein the predetermined responsive action includes adding information pertaining to the Downloadable to a suspicious Downloadables database.

* * * * *

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on December 10, 2013, a copy of the foregoing document:

**BRIEF FOR PLAINTIFF-APPELLANT
FINJAN, INC.**

was filed electronically with the Clerk of the Court using the Appellate CM/ECF System, which will send a Notice of Docket Activity via electronic mail to all counsel of record. Additionally, a copy of the foregoing document was served upon counsel for each of the Defendants-Appellees via electronic mail listed below:

Jack B. Blumenfeld
MORRIS NICHOLS ARCHT &
TUNNELL LLP
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19889
jblumenfeld@mnat.com
MNATSymantec_Finjan@mnat.com

*Attorneys for Defendant-Appellee
Symantec Corporation*

Thomas C. Grimm
MORRIS NICHOLS ARCHT &
TUNNELL LLP
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19889
tcgefiling@mnat.com
Websense_Finjan@mnat.com

*Attorneys for Defendant-Appellee
Websense Inc.*

Anthony M. Stiegler
COOLEY LLP
4401 Eastgate Mall
San Diego, CA 92121
tstiegler@cooley.com
Websense-Finjan@cooley.com

Attorneys for Defendant-Appellee
Websense Inc.

John Allcock
Kathryn Riley Grasso
Sean C. Cunningham
DLA PIPER LLP
401 B Street, Suite 1700
San Diego, CA 92101
john.allcock@dlapiper.com
kathryn.riley@dlapiper.com
sean.cunningham@dlapiper.com
sophos@dlapiper.com

Attorneys for Defendant-Appellee
Sophos Inc.

Denise Kraft
DLA Piper LLP
1201 N. Market Street, Suite 2100
Wilmington, DE 19801
denise.kraft@dlapiper.com

Attorneys for Defendant-Appellee
Sophos Inc.

Lori Mason
COOLEY LLP
3000 El Camino Real
Palo Alto, CA 94306
lmason@cooley.com

Attorneys for Defendant-Appellee
Websense Inc.

Jennifer A. Kash
Sean S. Pak
QUINN EMANUEL URQUHART &
SULLIVAN
50 California Street, 22nd Floor
San Francisco, CA 94111
jenniferkash@quinnemanuel.com
seanpak@quinnemanuel.com
Finjan-Symantec@quinnemanuel.com

Attorneys for Defendant-Appellee
Symantec Corp.

Dated: December 10, 2013

/s/ Paul J. Andre
Paul J. Andre

CERTIFICATE OF COMPLIANCE WITH RULE 32(A)

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 13,940 words, exclusive of the certificate of interest, table of contents, table of citations, statement of related cases, addendum and this certificate of compliance as exempted by Fed. R. App. 32(a)(7)(B)(iii) and Fed. Cir. R. 32(b).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2007 in Times New Roman 14 point font.

Dated: December 10, 2013

Respectfully submitted,

/s/Paul J. Andre
Paul J. Andre
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, California 94025
Tel: (650) 752-1700
Fax: (650) 752-1800

Attorneys For Plaintiff-Appellant
Finjan, Inc.